COMPENDIO DE DOCUMENTOS REGULATORIOS

2025 TELEMÁTICA E INFORMÁTICA

Dirección de Regulaciones

MINISTERIO DE COMUNICACIONES | Cuba

COMPENDIOS DE DOCUMENTOS REGULATORIOS

Telecomunicaciones y Uso Del Espectro Radioeléctrico

Servicios Telemáticos e Informática

Servicios Postales

Fecha de Actualización:
31/1/2025

COMPENDIO DE DOCUMENTOS REGULATORIOS

2025 TELEMÁTICA E INFORMÁTICA

Dirección de Regulaciones

MINISTERIO DE COMUNICACIONES | Cuba

“Planteada la lucha de ideas a nivel mundial, muchas veces no se tiene acceso a los medios de divulgación masiva controlados por las grandes transnacionales, o no se tiene acceso a las grandes cadenas de televisión o de información; pero siempre hay alguna forma de hacer llegar el mensaje al mundo, siempre hay alguna posibilidad, y mientras más se desarrollen las comunicaciones, ello es más posible”.

Discurso pronunciado por Fidel Castro Ruz en la clausura del evento internacional Economía'98, 3 de julio de 1998

Presentación

El Compendio de Documentos Regulatorios es la compilación de las normas jurídicas vigentes, que rigen las tres ramas fundamentales técnicas y de servicios en las que el Ministerio de Comunicaciones es el organismo rector.

El objetivo de este compendio es brindar a las personas interesadas de forma coherente y organizada, el marco regulatorio del Ministerio de Comunicaciones y que este sea de utilidad, no solo para los trabajadores del sector, sino también para todo aquel que desee consultarlo.

La recopilación, selección y organización de la documentación fue realizada por los especialistas de la Dirección de Regulaciones del Ministerio de Comunicaciones.

La información se presenta en tres libros: Servicios Postales, Telemática e Informática y Telecomunicaciones/TIC y Uso del Espectro Radioeléctrico, con el propósito de hacerlo práctico para el trabajo.

Deseamos que esta información sea de su interés y atenderemos las sugerencias que nos hagan llegar para tenerlas en cuenta en futuras ediciones.

Wilfredo López Rodríguez
Director de Regulaciones
Ministerio de Comunicaciones

Índice

1. NORMAS JURÍDICAS SUPERIORES

DECRETO-LEY No. 370/2018

MIGUEL DÍAZ-CANEL BERMÚDEZ, Presidente del Consejo de Estado de la República de Cuba.

HAGO SABER: Que el Consejo de Estado ha considerado lo siguiente:

POR CUANTO: La informatización de la sociedad en Cuba desempeña un papel significativo en el desarrollo político, económico y social del país y constituye un medio efectivo para la consolidación de las conquistas del Socialismo y el bienestar de la población.

POR CUANTO: Resulta de interés del estado cubano para elevar la soberanía tecnológica, en beneficio de la sociedad, la economía, la seguridad y defensa nacional; contrarrestar las agresiones cibernéticas, salvaguardar los principios de seguridad de nuestras redes y servicios; así como defender los logros alcanzados por el Estado Socialista, siendo necesario emitir la norma jurídica que regule la informatización de la sociedad en Cuba.

POR TANTO: El Consejo de Estado en el ejercicio de las atribuciones que le han sido conferidas en el inciso c), del Artículo 90 de la Constitución de la República de Cuba, adopta el siguiente:

DECRETO-LEY No. 370
"SOBRE LA INFORMATIZACIÓN DE LA SOCIEDAD EN CUBA"

TÍTULO I
OBJETO, OBJETIVOS, ORGANIZACIÓN INSTITUCIONAL, COMPETENCIAS Y ATRIBUCIONES

CAPÍTULO I
OBJETO Y OBJETIVOS

ARTÍCULO 1.- El Estado promueve el desarrollo y utilización de las Tecnologías de la Información y la Comunicación, con el objetivo de que constituyan una fuerza política, científica y económica, que contribuya y propicie la integración y conducción de los procesos asociados a la informatización de la sociedad.

ARTÍCULO 2.- La informatización de la sociedad es el proceso de aplicación ordenada y masiva de las Tecnologías de la Información y la Comunicación en la gestión de la información y el conocimiento, con la seguridad requerida, para satisfacer gradualmente las necesidades de todas las esferas de la vida social, en su esfuerzo por parte del Estado de lograr cada vez más eficacia y eficiencia en los procesos, así como mayor generación de riqueza y aumento de la calidad de vida de los ciudadanos.

ARTÍCULO 3.- Se denominan Tecnologías de la Información y la Comunicación, en lo adelante TIC, al conjunto de recursos, herramientas, equipos, programas y aplicaciones informáticas, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información en cualquier formato: voz, datos, texto, video e imágenes.

ARTÍCULO 4.- El presente Decreto-Ley es aplicable a las relaciones jurídicas relacionadas con las TIC y tiene como objeto establecer su marco legal, de tal forma que ordene y garantice el derecho al acceso y participación de las personas naturales y jurídicas en la informatización de la sociedad, en correspondencia con lo establecido en la Constitución, las leyes y las restantes disposiciones legales, así como los tratados y demás instrumentos jurídicos internacionales en la materia, de los que la República de Cuba es Estado parte.

ARTÍCULO 5.- Los objetivos del presente Decreto-Ley son los siguientes:

a) Fortalecer el proceso de informatización, en función de modernizar coherentemente todas las esferas de la sociedad y contribuir al desarrollo económico y social del país;
b) consolidar el uso y desarrollo de las TIC, como instrumento para la defensa de la Revolución;
c) promover y favorecer el acceso y el uso responsable de los ciudadanos a las TIC;
d) consolidar la defensa política y la ciberseguridad frente a las amenazas, los ataques y riesgos de todo tipo;
e) preservar y desarrollar los recursos humanos asociados a la actividad;
f) satisfacer las necesidades generales para incrementar el uso de las TIC y su aplicación por el Estado y del Gobierno, en la Seguridad y Defensa Nacional, y el Orden Interior;
g) favorecer el uso de las TIC en los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro y las organizaciones políticas, sociales y de masas;
h) asegurar la sostenibilidad y soberanía tecnológica de las TIC en función del desarrollo de la informatización del país; e
i) incentivar y promover la integración de la investigación, desarrollo e innovación con la producción y comercialización de equipos, programas y aplicaciones informáticas, contenidos y servicios asociados a las TIC.

CAPÍTULO II
ORGANIZACIÓN INSTITUCIONAL

ARTÍCULO 6.- La informatización de la sociedad cubana se garantiza por los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, según su misión y funciones específicas, con la contribución de las formas asociativas sin fines de lucro y las organizaciones políticas, sociales y de masas.

ARTÍCULO 7.- El Ministerio de Comunicaciones, en coordinación con los de las Fuerzas Armadas Revolucionarias y del Interior, es el responsable de orientar las tareas y acciones que garanticen la

informatización de la sociedad.

CAPÍTULO III
COMPETENCIAS Y ATRIBUCIONES

Sección Primera
Competencias del Ministerio de Comunicaciones respecto al proceso de informatización de la sociedad

ARTÍCULO 8.- El Ministerio de Comunicaciones es el organismo encargado de otorgar la autorización, entendida esta como la licencia concedida a una persona natural o jurídica en el ámbito de las TIC, para según las condiciones que en esta se establecen, proyectar, instalar, mantener y comercializar programas y aplicaciones informáticas o proveer un servicio relacionado con lo autorizado.

ARTÍCULO 9.- Es competencia del Ministerio de Comunicaciones, en el proceso de informatización de la sociedad, en colaboración con los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, las formas asociativas sin fines de lucro y las organizaciones políticas, sociales y de masas, de acuerdo con las prioridades económicas y sociales del país, y con su misión y funciones específicas:

a) Organizar, normar y estandarizar la actividad informática en los órganos y organismos del Estado y del Gobierno a todos los niveles que corresponda;
b) fomentar la producción de equipamiento vinculado a las TIC e incentivar su establecimiento en zonas especiales de desarrollo, en correspondencia con las prioridades de informatización del país;
c) coadyuvar al desarrollo y modernización de la infraestructura tecnológica, que permita un empleo eficiente de los recursos y garantice la seguridad, calidad y el acceso a los servicios de las TIC para toda la sociedad, así como el despliegue y desarrollo de infraestructuras tecnológicas en los sectores productivos y de servicios de impacto en la sociedad;
d) promover la integración ordenada de las redes institucionales y de uso público, en función del acceso a los servicios y que garantice su seguridad;
e) fomentar de forma racional un sistema de centros de datos con condiciones tecnológicas, respaldo y seguridad adecuados, como soporte al proceso de informatización y a las necesidades de las entidades que lo requieran;
f) potenciar el desarrollo de la infraestructura de telecomunicaciones, en especial el despliegue de la banda ancha, para garantizar su cobertura nacional y ampliar la capilaridad en la red de acceso, fundamentalmente con el empleo de tecnologías inalámbricas que incluye la móvil;
g) participar en el diseño e implementación del sistema de gestión integrada del capital humano del sector de las TIC;
h) impulsar la cooperación internacional, en función de fortalecer el desarrollo de las TIC y la participación del país en foros internacionales y multilaterales, que permitan la adopción de estándares para el desarrollo de las TIC;
i) establecer convenios y alianzas que contribuyan al desarrollo de soluciones, al acceso,

transferencias de tecnologías y al desarrollo del capital humano;

j) promover el desarrollo y la implementación de los servicios en línea entre las instituciones y hacia los ciudadanos, con prioridad en los servicios y trámites de la población, la gestión del gobierno y el comercio electrónico;
k) conducir la elaboración de los planes para el desarrollo y uso de las TIC en cada sector de la economía, con prioridad en aquellos que sean estratégicos, así como a nivel territorial;
l) apoyar el fortalecimiento de las entidades especializadas en las TIC, de manera que haya una mayor integración y mejor conducción de los procesos asociados a la informatización de la sociedad, así como crear alianzas entre las diferentes empresas y las entidades de ciencia, tecnología e innovación del país para alcanzar los objetivos estratégicos que se proponga la nación;
m) garantizar el diseño e instrumentación de un sistema que perfeccione, armonice y desarrolle el marco legal que sustente el proceso de informatización de la sociedad, así como el control y fiscalización de su cumplimiento; y
n) coadyuvar a que los procesos de informatización se desarrollen con un análisis organizacional y con un enfoque sistémico integrado.

Sección Segunda
Competencias de los órganos, organismos y entidades nacionales del Estado y del Gobierno en el proceso de informatización de la sociedad

ARTÍCULO 10.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, de acuerdo con su misión y funciones específicas aprobadas, desarrollan las acciones que se establecen mediante el presente Decreto-Ley, en el marco del proceso de informatización de la sociedad cubana.

ARTÍCULO 11.- El ministro de Comunicaciones propone al Consejo de Ministros para su aprobación con la participación del Ministerio de Economía y Planificación, el Programa Nacional de Informatización, que integre y armonice por cada sector y a nivel territorial, las principales prioridades del país a corto, mediano y largo plazos a los fines de su incorporación a los planes de la economía del país y una vez aprobado realiza su implementación así como establece los indicadores de dicho Programa que puedan medir su impacto.

ARTÍCULO 12.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular son los responsables de implementar en sus planes las actividades que le correspondan dentro del Programa Nacional de Informatización, y su aseguramiento económico.

TÍTULO II
DESARROLLO DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

CAPÍTULO I
INDUSTRIA CUBANA DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

ARTÍCULO 13.- Se entiende por programa y aplicación informática, conocido como software, al programa de computación o conjunto de estos, procedimientos y posible documentación y datos asociados; entre los que se encuentran:

a) Programa y aplicación informática de código abierto: es aquel que posee licencia y permite, con mayores o menores restricciones, ejecutar, modificar y distribuir la aplicación informática, brinda acceso a sus programas listados de códigos fuente, con reconocimiento o no del autor.
b) Programa y aplicación informática propietario, también llamado software no libre, software privativo, software privado, software propietario o software de propiedad: es aquel en el que los usuarios tienen limitadas las posibilidades de usarlo, modificarlo o redistribuirlo, con o sin modificaciones, o cuyo código fuente no está disponible o el acceso a éste se encuentra restringido.

ARTÍCULO 14.- El alcance de la industria de programas y aplicaciones informáticas, en lo adelante la Industria, comprende a las entidades y al trabajador por cuenta propia, cuya función, objeto social o actividad económica autorizada es el desarrollo de programas y aplicaciones informáticas y la prestación de servicios informáticos asociados a esta industria.

ARTÍCULO 15.- El Ministerio de Comunicaciones organiza, coordina y promueve la Industria, en correspondencia con las prioridades de informatización del país, orientadas a fortalecer la soberanía tecnológica, la sustitución de importaciones y el incremento de exportaciones.

ARTÍCULO 16.- Corresponde al Ministerio de Comunicaciones implementar el sistema de control administrativo de inscripción de los programas y aplicaciones informáticas y servicios asociados a las TIC, que se pretendan comercializar, así como sus desarrolladores.

ARTÍCULO 17.- El Ministerio de Comunicaciones adopta las acciones necesarias, en coordinación con los organismos competentes, para incrementar la producción nacional y las exportaciones de programas y aplicaciones informáticas de la Industria.

ARTÍCULO 18.- El Ministerio de Comunicaciones, en coordinación con los organismos competentes para perfeccionar los mecanismos de gestión, actualización, socialización y comercialización de servicios, contenidos digitales y dispositivos informáticos adopta las acciones necesarias en cuanto a:

a) Establecer una plataforma nacional que incentive la generación de contenidos y garantice la

posibilidad de socializarlos, dirigidos a fortalecer la identidad, el respeto y el conocimiento a la cultura e historia nacional, así como a preservar los valores de la sociedad cubana;

b) promover la ampliación de capacidades y el uso de Internet, con precios cada vez más accesibles y competitivos;
c) controlar que se establezcan modelos de negocios entre el operador de redes de telecomunicaciones y los proveedores de servicios, programas
d) y aplicaciones informáticas, de manera que se estimule la producción de contenidos y servicios digitales nacionales; y
e) favorecer que se implemente una estrategia de precios asequible para la comercialización de los dispositivos informáticos, la producción de aplicaciones y contenidos, así como el uso racional de la infraestructura.

ARTÍCULO 19.- El Ministerio del Comercio Exterior y la Inversión Extranjera en coordinación con el de Comunicaciones, establece e implementa la estrategia para la exportación de programas y aplicaciones informáticas, servicios y contenidos digitales.

ARTÍCULO 20.- Los ministerios de Cultura y el de Ciencia, Tecnología y Medio Ambiente, en lo referido al derecho de autor y a la propiedad intelectual respectivamente, en coordinación con el Ministerio de Comunicaciones, establecen las normas para la protección a los autores y titulares de programas y aplicaciones informáticas, a partir de las necesidades del desarrollo científico y tecnológico del país en la explotación de este tipo de creación, así como los mecanismos que garanticen la protección del patrimonio nacional.

ARTÍCULO 21.- El Ministerio de Comunicaciones, con la participación del de Economía y Planificación, establece el diseño económico, que permita aumentar y diversificar las fuentes de financiamiento, en respaldo a la modernización de la infraestructura tecnológica, así como a las prioridades del Programa Nacional de Informatización.

ARTÍCULO 22.- Los operadores de redes de telecomunicaciones y los proveedores de servicios TIC, garantizan la oferta de tarifas preferenciales para impulsar las capacidades tecnológicas de las entidades de programas y aplicaciones y servicios informáticos; de igual manera, los suministradores de equipamiento informático establecen precios preferenciales, comparables a los internacionales, a las entidades que desarrollan programas y aplicaciones informáticas y servicios informáticos.

CAPÍTULO II
PROGRAMAS Y APLICACIONES INFORMÁTICAS DE CÓDIGO ABIERTO

ARTÍCULO 23.- El Estado promueve la utilización de programas y aplicaciones informáticas que utilicen plataformas de código abierto y de producción nacional, con el objetivo de priorizar su uso e incrementar la soberanía tecnológica y la seguridad nacional.

ARTÍCULO 24.- El Ministerio de Comunicaciones es el responsable de elaborar, establecer y controlar el plan para la migración de programas y aplicaciones informáticas propietarios, hacia plataformas de

código abierto de producción nacional, en coordinación con los órganos y organismos de la Administración Central del Estado y el Banco Central de Cuba, así como adoptar las medidas que garanticen brindar servicios de asesoría técnica, formación del personal y acceso a las aplicaciones de código abierto.

ARTÍCULO 25.- La migración de programas y aplicaciones informáticas propietarios hacia plataformas de código abierto y de producción nacional, se aplica a los órganos, organismos de la Administración Central del Estado y el Banco Central de Cuba; esta migración se realiza de forma ordenada y progresiva y donde sea imprescindible coexiste con los sistemas propietarios, siempre que satisfagan los requerimientos de seguridad y las necesidades de informatización de cada entidad.

TÍTULO III
GOBIERNO Y COMERCIO ELECTRÓNICO

CAPÍTULO I
GOBIERNO ELECTRÓNICO

ARTÍCULO 26.- El Estado incorpora el Gobierno Electrónico en la prestación de sus servicios y trámites, la difusión de información e interacción con la población.

ARTÍCULO 27.- El Gobierno Electrónico es el uso de las TIC en la gestión de la administración pública para incrementar su eficacia y eficiencia, con la finalidad de mejorar la información y los servicios ofrecidos a los ciudadanos, incrementar la transparencia del sector público y la participación de la población.

ARTÍCULO 28.- El Ministerio de Comunicaciones, en coordinación con otros órganos, organismos de la Administración Central del Estado y el Banco Central de Cuba, elabora las propuestas de acciones para implementar el Gobierno Electrónico.

ARTÍCULO 29.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, aplican las acciones aprobadas para establecer el Gobierno Electrónico, con el objetivo de garantizar el máximo aprovechamiento de las TIC y la prestación de servicios eficientes a la población.

ARTÍCULO 30.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular que tengan a su cargo Registros Públicos, son responsables de su informatización y de priorizar su ejecución.

ARTÍCULO 31.- Los documentos en formato digital firmados electrónicamente con el empleo de certificados digitales de la Infraestructura Nacional de Llave Pública, conforme a las regulaciones establecidas por la Ley, prueban la autenticidad de la elaboración de éstos y son reconocidos como válidos, con plena eficacia por las autoridades y funcionarios públicos a todos los efectos procedentes.

ARTÍCULO 32.- El Ministro de Justicia, en el marco de su competencia, con la colaboración de los ministerios del Interior y de Comunicaciones y demás órganos y organismos de la Administración Central del Estado, que correspondan, propone, o emite en su caso, las disposiciones jurídicas que resulten necesarias para dotar de validez legal los documentos en formato digital.

ARTÍCULO 33.- Los datos de carácter personal en soporte electrónico, solo se pueden revelar a terceros que posean interés legítimo debidamente acreditado ante autoridad competente o que estén autorizado por el titular de estos datos; ante el incumplimiento de lo dispuesto, se procede conforme a lo establecido en la legislación vigente.

ARTÍCULO 34.- El Jefe de la Oficina Nacional de Estadísticas e Información, en coordinación con el Ministerio de Comunicaciones establece los procedimientos, normativas y estándares tecnológicos que garanticen la interoperabilidad de la información a nivel nacional y la comparabilidad en el ámbito internacional.

ARTÍCULO 35.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular determinan los servicios que brindan a la población, facilitan y optimizan los trámites y el acceso a la información, así como la atención ciudadana en línea, y son responsables del uso de las plataformas tecnológicas que protejan los datos del usuario y garanticen la veracidad y autenticidad de la información.

ARTÍCULO 36.- Los ministerios de Educación y Educación Superior incluyen temáticas de Gobierno Electrónico en los planes de estudio en todos los niveles de enseñanza, según corresponda.

ARTÍCULO 37.- Las entidades aportan, en el ejercicio de sus funciones, los recursos materiales y humanos, así como la capacitación necesaria para el desarrollo y uso de las TIC.

CAPÍTULO II
COMERCIO ELECTRÓNICO

ARTÍCULO 38.- El Comercio Electrónico es la actividad comercial que se desarrolla mediante la utilización de las TIC que comprende promoción, negociación de precios y condiciones de contratación, facturación y pago, entrega de bienes o servicios, así como servicios de posventa, entre otros.

ARTÍCULO 39.- Corresponde al Ministerio del Comercio Interior, con la participación de los de Comercio Exterior y la Inversión Extranjera, y de Comunicaciones, y en coordinación con los organismos mencionados en los artículos 43 y 44, desarrollar las acciones para implementar el Comercio Electrónico, así como la exportación e importación de bienes y servicios vinculados a este.

ARTÍCULO 40.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular y el sistema empresarial, de acuerdo con sus funciones, crean las condiciones para el desarrollo y la participación en el Comercio Electrónico y realizan actividades de capacitación a los directivos, técnicos y especialistas en esta esfera.

ARTÍCULO 41.- Las personas naturales y jurídicas que participen en actividades de Comercio Electrónico han de cumplir con la legislación vigente en materia de comercio.

ARTÍCULO 42.- Las personas naturales y jurídicas que provean bienes y servicios por medios digitales, están obligadas a desarrollar un entorno técnicamente seguro para las transacciones comerciales en las que operan, de acuerdo con la legislación vigente.

ARTÍCULO 43.- Corresponde a los órganos y organismos de la Administración Central del Estado, implementar en el marco de su competencia, las acciones y medidas siguientes:

a) El Ministerio de Comunicaciones garantiza que los proveedores de servicios brinden la conectividad necesaria con la debida seguridad, para desarrollar el Comercio Electrónico en el país;
b) el Ministerio de Economía y Planificación prioriza, según las condiciones existentes, los recursos a destinar por el sistema empresarial para la seguridad, supervisión y desarrollo del Comercio Electrónico;
c) el Ministerio de Justicia con la participación de los del Comercio Exterior y la Inversión Extranjera, y del Comercio Interior, aprueba las disposiciones jurídicas que resulten necesarias para el intercambio de los documentos en formato digital, relacionados con el Comercio Electrónico;
d) el Ministerio del Transporte realiza los estudios y establece las normas para garantizar los servicios de transportación asociados al Comercio Electrónico;
e) el Ministerio del Comercio Interior, en el marco de su competencia, establece las disposiciones normativas para garantizar el adecuado desarrollo del Comercio Electrónico y las medidas de seguridad, así como los procedimientos de control necesarios;
f) el Ministerio de Cultura establece las disposiciones que le correspondan, acerca de la Protección de los Derechos de Autor sobre obras intelectuales que se comercializan a través del Comercio Electrónico; y
g) los ministerios de Educación y Educación Superior incluyen temáticas de Comercio Electrónico en los planes de estudio en todos los niveles de enseñanza, según corresponda.

ARTÍCULO 44.- El Banco Central de Cuba evalúa y autoriza los instrumentos de pagos y sus proveedores de servicios, las infraestructuras, y los mecanismos para el procesamiento de los pagos por vía electrónica.

TÍTULO IV
SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LA DEFENSA NACIONAL

CAPÍTULO I
SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

ARTÍCULO 45.- El Estado identifica las Infraestructuras Críticas de las TIC y su seguridad y protección para su correcto funcionamiento.

ARTÍCULO 46.- Las Infraestructuras Críticas de las Tecnologías de la Información y la Comunicación son aquellas que soportan los componentes, procesos y servicios esenciales que garanticen las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública.

ARTÍCULO 47.- El Ministerio de Comunicaciones, en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, establece el Programa para el Fortalecimiento de la Ciberseguridad y coordina la participación en las actividades internacionales requeridas a ese fin, e implementa su control y fiscalización.

ARTÍCULO 48.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, implementan las acciones que se corresponden con la política y estrategias de seguridad de las TIC aprobadas, que se establecen en el programa para su fortalecimiento; entre estas acciones se tienen en cuenta:

a) Las soluciones y la infraestructura que garanticen la autenticación, seguridad, legitimidad y autenticidad para el proceso de informatización del país;
b) la seguridad de los sistemas tecnológicos que procesan información clasificada o sirven de sustento a las Infraestructuras Críticas de las TIC,
c) la investigación, desarrollo, asimilación tecnológica y soporte de soluciones para la seguridad de las TIC de forma sostenible;
d) el perfeccionamiento del proceso de compatibilización de los servicios, tecnologías e inversiones con los órganos de la defensa;
e) la certificación y supervisión de las soluciones, servicios y la infraestructura tecnológica; y
f) la actividad de gestión, control, fiscalización y actuación ante incidentes de la seguridad de las TIC.

ARTÍCULO 49.- Las personas naturales, usuarios de las TIC, cumplen en lo que a ellas corresponde, con el programa vigente de fortalecimiento de la seguridad de las TIC.

CAPÍTULO II
DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN PARA LA SEGURIDAD Y LA DEFENSA NACIONAL

ARTÍCULO 50.- El Ministerio de Comunicaciones, con la participación de los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, coordina y establece las acciones que permitan mejorar paulatinamente las condiciones de fiabilidad, estabilidad y el uso seguro de las TIC, para respaldar la seguridad y la defensa nacional, de forma paralela con la informatización de la sociedad.

ARTÍCULO 51.- Los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, definen los requerimientos técnicos, organizativos y de seguridad de los servicios de interés para el país, soportados en sus infraestructuras tecnológicas.

ARTÍCULO 52.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, organizan sus servicios de las TIC en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, para responder a las necesidades que el país requiera en situaciones excepcionales y las vinculadas a la seguridad y la defensa nacional.

TÍTULO V
INVESTIGACIÓN, DESARROLLO, INNOVACIÓN TECNOLÓGICA Y CAPITAL HUMANO

CAPÍTULO I
INVESTIGACIÓN, DESARROLLO E INNOVACIÓN TECNOLÓGICA

ARTÍCULO 53.- Corresponde al Ministerio de Ciencia, Tecnología y Medio Ambiente en coordinación con los de Educación Superior y de Comunicaciones, establecer un programa de ciencia, tecnología e innovación de las TIC que aproveche las potencialidades del capital humano, en especial las universidades y centros de investigación.

ARTÍCULO 54.- Los ministerios de Ciencia, Tecnología y Medio Ambiente y de Comunicaciones, en coordinación con los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, establecen los programas de ciencia, tecnología e innovación y las acciones que promuevan la investigación científica e industrial en esta especialidad, de conformidad con los objetivos del presente Decreto-Ley.

ARTÍCULO 55.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, implementan las acciones que se corresponden con el programa vigente de ciencia, tecnología e innovación de las TIC y garantizan el acceso a Internet de los profesionales.

ARTÍCULO 56.- El Ministerio de Industrias en coordinación con el de Comunicaciones, diseña la estrategia para reducir gradualmente la obsolescencia tecnológica, con sus planes de producción y sostenibilidad, a partir de las prioridades de informatización de la sociedad.

CAPÍTULO II
CAPITAL HUMANO

ARTÍCULO 57.- El Ministerio de Comunicaciones fomenta programas de calificación y adiestramiento, a fin de ampliar y actualizar la especialización en las diferentes ramas de las TIC, con especial énfasis en la ciberseguridad, los programas y aplicaciones informáticas de código abierto, el desarrollo técnico y profesional, así como los programas de apoyo a la educación tecnológica, en coordinación con las instituciones de educación media y superior del país.

ARTÍCULO 58.- Los ministerios de Educación y Educación Superior en coordinación con el de Comunicaciones, desarrollan acciones que:

a) Impulsen la investigación, desarrollo, innovación y producción en las TIC y contribuyan a implementar la introducción de los resultados obtenidos;
b) implementan modelos educativos en todos los niveles de enseñanza, que generen el capital humano con las capacidades para desarrollar, sostener y utilizar las TIC; y
c) desarrollen los programas de capacitación en las diferentes ramas de las TIC, acorde con su complejidad y evolución tecnológica.

ARTÍCULO 59.- Los ministerios de Comunicaciones y de Trabajo y Seguridad Social, de acuerdo con sus funciones, desarrollan acciones encaminadas a:

a) Actualizar periódicamente los calificadores y jerarquizar los cargos, a partir de la idoneidad demostrada para los diferentes perfiles y el conocimiento real, con la participación de la organización sindical del nivel correspondiente;
b) perfeccionar el proceso de planificación de la formación, así como la demanda y distribución de la fuerza de trabajo calificada; y
c) desarrollar el teletrabajo en coordinación con los demás órganos y organismos de la Administración Central del Estado.

TÍTULO VI
REGULACIÓN, CONTROL Y FISCALIZACIÓN DEL PROCESO DE INFORMATIZACIÓN EN LA SOCIEDAD CUBANA

CAPÍTULO I
REGULACIÓN, CONTROL Y FISCALIZACIÓN

ARTÍCULO 60.- El Ministerio de Comunicaciones, con la participación de los del Interior y las Fuerzas Armadas Revolucionarias, designa las unidades organizativas y entidades que garanticen la regulación, control y fiscalización para asegurar el cumplimiento de lo que establece el presente Decreto-Ley.

ARTÍCULO 61.- Todo proveedor de servicios públicos de las TIC tiene que brindar al Ministerio de Comunicaciones la información que éste determine para el cumplimiento de sus funciones.

ARTÍCULO 62.- Corresponde a los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, las formas asociativas sin ánimos de lucro, las cooperativas y las organizaciones políticas, sociales y de masas, instrumentar el proceso de informatización en su esfera de actividades e implementar el control y fiscalización que corresponda.

ARTÍCULO 63.- La Contraloría General de la República con la participación de los ministerios del Interior, de Finanzas y Precios y de Comunicaciones establece las Directrices para el desarrollo de la auditoría a las TIC y la evaluación del Sistema de Control Interno asociado a estas y a la actividad de Comercio Electrónico.

ARTÍCULO 64.- Las personas naturales y jurídicas sometidas al control y fiscalización en la esfera de las TIC, colaboran y facilitan la gestión de los funcionarios de las correspondientes entidades o unidades organizativas encargadas de estas funciones, sin perjuicio de los derechos constitucionalmente reconocidos.

ARTÍCULO 65.- Las autoridades de orden público prestan la protección y auxilio a los funcionarios de las correspondientes entidades o unidades organizativas de control y fiscalización en la esfera de las TIC.

CAPÍTULO II
MEDICIÓN DEL PROCESO DE INFORMATIZACIÓN EN LA SOCIEDAD CUBANA

ARTÍCULO 66.- Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular realizan mediciones de los impactos del proceso de informatización, para lo que tienen en cuenta, entre otros la reducción de gastos, la optimización de la fuerza de trabajo y la calidad del servicio o producto.

ARTÍCULO 67.- La Oficina Nacional de Estadísticas e Información:

a) Incluye en el Sistema de Información Estadístico Nacional los indicadores, definiciones metodológicas y procedimientos de control, de la informatización de la sociedad; y
b) con la colaboración de los ministerios de Comercio Exterior y la Inversión Extranjera, del Comercio Interior y de Economía y Planificación, establece los procedimientos de control estadísticos, los indicadores sobre los bienes y servicios que se comercialicen electrónicamente y sus definiciones metodológicas.

TÍTULO VII
CONTRAVENCIONES Y SANCIONES ASOCIADAS A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LOS RECURSOS ADMINISTRATIVOS PARA SU IMPUGNACIÓN

CAPÍTULO I
DE LAS CONTRAVENCIONES Y SANCIONES ASOCIADAS A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

ARTÍCULO 68.- Se consideran contravenciones asociadas a las TIC, siempre que no constituyan delitos, las violaciones siguientes:

a) Comercializar programas, aplicaciones y servicios informáticos asociados a estos sin la autorización del organismo competente de acuerdo con la legislación vigente;
b) fabricar, comercializar, transferir, instalar equipos y demás dispositivos para brindar, facilitar o recibir servicios asociados a las TIC, sin la correspondiente autorización;
c) diseñar, distribuir o intercambiar códigos de virus informáticos u otros programas malignos entre personas naturales o jurídicas; se exceptúa la información enviada por usuarios a la autoridad competente para su análisis e investigación;
d) adicionar algún equipo de telecomunicaciones/TIC o introducir cualquier tipo de programas y aplicaciones informáticas en una red de datos, ya sea a través de soportes removibles o mediante acceso a redes externas sin la autorización del titular o no garantizar su compatibilización con las medidas de seguridad establecidas para la protección de la red de datos;
e) acceder sin la autorización o agredir a cualquier sistema de cómputo conectado a las redes públicas de transmisión de datos y la usurpación de los derechos de acceso de usuarios debidamente autorizados;
f) hospedar un sitio en servidores ubicados en un país extranjero, que no sea como espejo o réplica del sitio principal en servidores ubicados en territorio nacional;
g) interferir, interceptar, alterar, dañar o destruir datos, información, soportes informáticos, programas o sistemas de información y comunicación de servicios públicos, sociales y administrativos;
h) realizar acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros, sin la debida autorización; y

i) difundir, a través de las redes públicas de transmisión de datos, información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas.

CAPÍTULO II
DE LAS SANCIONES ACCESORIAS

ARTÍCULO 69.- A la persona natural que contravenga lo dispuesto en los incisos a), e) y f) del Artículo 68 se le impone una multa de mil pesos ($ 1 000 CUP); en caso de ser una persona jurídica, la multa que se le impone es de cinco mil pesos ($5 000 CUP).

ARTÍCULO 70.- A la persona natural que contravenga lo dispuesto en los restantes incisos del Artículo 68, se le impone una multa de tres mil pesos ($3 000 CUP); en caso de ser una persona jurídica, la multa que se le impone es de diez mil pesos ($10 000 CUP).

ARTÍCULO 71.- A los responsables de la comisión de contravenciones establecidas por el presente Decreto-Ley y sus disposiciones complementarias, además de la sanción de multa se le puede imponer las accesorias siguientes:

a) Decomiso de los equipos y medios utilizados para cometer las contravenciones previstas en el artículo 68;
b) suspensión de la licencia de forma temporal o la cancelación definitiva; y
c) clausura de las instalaciones.

ARTÍCULO 72.- Las acciones administrativas por parte de la autoridad facultada para exigir responsabilidad por las contravenciones reguladas en este Decreto-Ley se aplica inmediatamente a partir que se detectan y se identifique el comisor.

ARTÍCULO 73.- Las sanciones previstas en el presente Decreto-Ley se aplican sin perjuicio de la responsabilidad civil, penal, material u otra que puedan ser exigibles.

ARTÍCULO 74.- Los equipos y medios decomisados, pasan sin derecho a pago alguno al dominio del Ministerio de Comunicaciones.

ARTÍCULO 75.- Se faculta al Ministro de Comunicaciones a reglamentar el procedimiento y destino de los equipos y medios decomisados.

ARTÍCULO 76.- Contra las sanciones previstas en el presente Decreto-Ley se cumple lo establecido en la legislación vigente. No procede la reclamación por los beneficios dejados de percibir a resultas de los daños o perjuicios que pudieran ocasionarse por las medidas aplicadas.

CAPÍTULO III
DE LAS AUTORIDADES FACULTADAS PARA LA IMPOSICIÓN DE SANCIONES

ARTÍCULO 77.- Los inspectores designados por el Ministerio de Comunicaciones y por las administraciones locales del Poder Popular, quedan facultados para imponer la sanción de multa establecida; además de proponer y asistir en la aplicación del decomiso una vez aprobado por la autoridad facultada designada por el Ministerio de Comunicaciones, a los que infrinjan lo dispuesto en el presente Decreto-Ley y sus disposiciones complementarias.

ARTÍCULO 78.- Los inspectores designados por el Ministerio de Comunicaciones y por las administraciones locales del Poder Popular, quedan facultados para realizar la retención de los objetos sujetos a decomiso, a fin de garantizar su conservación y custodia, previo inventario e inician el expediente correspondiente; en los casos que así se requiera, son auxiliados en sus actuaciones por la Policía Nacional Revolucionaria.

CAPÍTULO IV
DE LOS RECURSOS Y PLAZOS DE PRESCRIPCIÓN

Sección Primera
Del Recurso de Apelación y Reforma

ARTÍCULO 79.- Contra las sanciones de multas impuestas por los inspectores a que se refieren los artículos anteriores, cabe la presentación de Recurso de Apelación ante en jefe de la entidad o unidad organizativa de control y fiscalización del área bajo jurisdicción y competencia, en el plazo de quince días hábiles, contados a partir de la fecha de su notificación, el que lo resuelve en el plazo de hasta sesenta días hábiles.

ARTÍCULO 80.- Procede el Recurso de Reforma ante el jefe de la entidad o o unidad organizativa de control y fiscalización del área bajo jurisdicción y competencia en el plazo de quince días hábiles, contados a partir de su notificación, contra la sanción de decomiso impuesta por la referida autoridad, quien lo resuelve en el plazo de sesenta días hábiles, contados a partir de su interposición.

ARTÍCULO 81.- El jefe de la entidad o unidad organizativa de control y fiscalización puede declarar inadmisibles los Recursos de Apelación y Reforma cuando estos se presenten fuera de los términos establecidos. Contra la decisión del jefe de la entidad o unidad organizativa de control y fiscalización procede Recurso de Alzada.

Sección Segunda
Del Recurso de Alzada

ARTÍCULO 82.- Contra la resolución que desestime en todo o en parte el Recurso de Apelación o Reforma, según el caso, interpuesto en primera instancia ante el jefe de la entidad o unidad organizativa de control y fiscalización del área bajo su jurisdicción y competencia, procede Recurso de Alzada ante el Ministro de Comunicaciones, en el plazo de quince días hábiles contados a partir de la notificación de la resolución anterior.

ARTÍCULO 83.- El Recurso de Alzada es resuelto por el Ministro de Comunicaciones en el plazo de hasta sesenta días hábiles contados a partir de su interposición; contra esta decisión no cabe recurso alguno por vía administrativa.

ARTÍCULO 84.- El ministro de Comunicaciones puede declarar inadmisible el Recurso de Alzada cuando este se presente extemporáneo.

ARTÍCULO 85.- Contra la resolución que resuelve el Recurso de Alzada, solo procede interponer en un término de treinta días, contado a partir de la notificación de aquella, demanda administrativa en la vía judicial, de acuerdo con el procedimiento establecido en la legislación de procedimiento civil, administrativo, laboral y económico.

ARTÍCULO 86.- Las resoluciones que resuelven los recursos de Apelación, de Reforma y de Alzada, se hacen firmes una vez decursado el término legalmente establecido para impugnarlas en la vía administrativa o judicial, según sea el caso; sin perjuicio del Procedimiento de Revisión, que se establece en la presente.

ARTÍCULO 87.- El Ministro de Comunicaciones excepcionalmente puede revisar de oficio o por solicitud del reclamante la decisión adoptada y revocarla, antes de que se haya establecido proceso en la vía judicial, siempre que la decisión sea favorable a la persona reclamante.

El Procedimiento de Revisión expresado en el párrafo anterior, procede cuando existan de hechos o pruebas demostrativas que no pudieron ser presentadas en el momento procesal oportuno y que resulten trascendentes al fondo del asunto, o se demuestre que la resolución impugnada infringe la ley por ser improcedente, arbitraria o ilegal.

Sección Tercera
De los plazos de prescripción

ARTÍCULO 88.- La acción administrativa por parte de la autoridad facultada para exigir responsabilidad por las contravenciones reguladas en este Decreto-Ley prescribe transcurrido un año después de su detección y no haber sido identificado el comisor.

ARTÍCULO 89.- El plazo para la aplicación de las multas, el decomiso u demás medidas por la

autoridad facultada, previstas en los artículos 69, 70 y 71 del presente Decreto-Ley, prescriben al año si no se ejecutan.

El término de prescripción se interrumpe por cualquier acción realizada por la citada autoridad, tendente a hacerla efectiva.

Después de cada interrupción, el término de prescripción comienza a decursar nuevamente.

DISPOSICIONES ESPECIALES

PRIMERA: Se faculta al Ministro de Comunicaciones para dictar en el ámbito de su competencia, las disposiciones jurídicas que correspondan para la aplicación de lo establecido en el presente Decreto-Ley.

SEGUNDA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior, a adecuar para sus sistemas, lo establecido en el presente Decreto-Ley, de conformidad con sus estructuras.

DISPOSICIONES FINALES

PRIMERA: El Consejo de Ministros queda encargado de dictar las disposiciones complementarias sobre la Industria de Programas y Aplicaciones Informáticas y sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional.

SEGUNDA: Los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en el marco de su competencia dictan las disposiciones legales, realizan el control y fiscalización, y establecen las coordinaciones que resulten necesarias, relativas a la aplicación del presente Decreto-Ley.

TERCERA: El glosario de términos y definiciones anexo al presente Decreto-Ley para su mejor comprensión, forma parte de su contenido.

CUARTA: Derogar las disposiciones siguientes:

1) Acuerdo No. 5586 de 26 de diciembre de 2005 del Consejo de Ministros, que aprueba los Lineamientos para el desarrollo en Cuba del Comercio Electrónico; y
2) Acuerdo No. 6058 de 9 de julio de 2007 del Comité Ejecutivo del Consejo de Ministros, que aprueba los Lineamientos de Seguridad de las tecnologías de la información.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, en La Habana, a los 17 días del mes de diciembre de 2018.

Miguel Díaz-Canel Bermúdez
Presidente del Consejo de Estado

ANEXO

GLOSARIO DE TÉRMINOS Y DEFINICIONES

1) Documento en formato digital: Es un tipo de contenido que proporciona información o datos, que puede ser procesado, trasmitido o almacenado y tiene la capacidad de proporcionar información de una persona a otra.
2) Entidad: Todos los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro y las organizaciones políticas, sociales y de masas.
3) Operador de redes de telecomunicaciones: Persona jurídica a la que se le otorga una concesión administrativa o autorización, de acuerdo con la legislación vigente, para la instalación, operación, explotación, mantenimiento y comercialización de redes de telecomunicaciones, para ofrecer servicios públicos de telecomunicaciones a usuarios finales.
4) Órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular: Todos los órganos superiores del Estado y del Gobierno, los órganos locales del Poder Popular, los organismos de la Administración Central del Estado, las organizaciones superiores de dirección empresarial que incluye a la Empresa de Telecomunicaciones de Cuba S.A.
5) Proveedor de servicios públicos de las TIC: Persona natural o jurídica, autorizada para prestar servicios de las TIC a terceros.
6) Servicios de las TIC: Son aquellos servicios de provisión de hospedaje y alojamiento; de aplicaciones; y de servicios informáticos.

DECRETO No. 360/2019

MIGUEL DÍAZ-CANEL BERMÚDEZ, Presidente de los consejos de Estado y de Ministros de la República de Cuba.

HAGO SABER: Que el Consejo de Ministros ha considerado lo siguiente:

POR CUANTO: El Decreto-Ley No. 370 "Sobre la Informatización de la Sociedad en Cuba", del 17 de diciembre del 2018, en su Disposición Final Primera establece que el Consejo de Ministros queda encargado de dictar las disposiciones complementarias sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional.

POR CUANTO: El referido Decreto-Ley No. 370, dispone las regulaciones generales aplicables a las Tecnologías de la Información y la Comunicación (TIC) y recoge los principios a seguir y las acciones y medidas para la determinación, desarrollo y mejoramiento de las condiciones de fiabilidad, estabilidad y seguridad de las TIC que respalden la informatización de la sociedad y la soberanía de la nación, la investigación, el desarrollo, la asimilación tecnológica y los soportes de soluciones para su seguridad de forma sostenible; acciones que requieren ser implementadas mediante las normas complementarias que resulten necesarias.

POR TANTO: El Consejo de Ministros, en el ejercicio de las atribuciones que le están conferidas en el Artículo 137, incisos ñ) y o) de la Constitución de la República de Cuba, dicta el siguiente:

DECRETO No. 360

SOBRE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LA DEFENSA DEL CIBERESPACIO NACIONAL

CAPÍTULO I
OBJETO, OBJETIVOS, DEFINICIONES Y ÁMBITO DE APLICACIÓN

Artículo 1. El Estado moviliza los recursos necesarios para lograr el empleo seguro y eficiente de las Tecnologías de la Información y la Comunicación en función de las necesidades que requiere el desarrollo del país; además, en su papel rector de la sociedad, dirige la implementación de la estrategia aprobada en materia de Seguridad de las Tecnologías de la Información y la Comunicación y controla su cumplimiento, así como promueve la investigación, el desarrollo, la aplicación, la innovación, la divulgación y la capacitación.

Artículo 2. El objeto del presente Decreto es establecer el marco legal que ordene el empleo seguro de las Tecnologías de la Información y la Comunicación, en lo adelante TIC, para la informatización de la sociedad, la defensa del Ciberespacio Nacional en correspondencia con lo establecido en la Constitución, las leyes y las restantes disposiciones legales relacionadas con el tema, así como los

tratados y demás instrumentos jurídicos internacionales de los que la República de Cuba es Estado parte.

Artículo 3. El objetivo general de este Decreto es establecer los niveles de seguridad en correspondencia con los riesgos asociados a la evolución de las TIC y las posibilidades reales de enfrentar estos últimos, y tiene los objetivos específicos siguientes:

a) Proteger el Ciberespacio Nacional y preservar la soberanía sobre su utilización;
b) establecer la seguridad de las TIC y de los servicios y aplicaciones que soportan; así como la de las Infraestructuras Críticas de las TIC con la finalidad de contar con una estrategia de fortalecimiento y sostenibilidad.

Artículo 4. El Ciberespacio es el ambiente virtual y dinámico, definido por tecnologías, equipos, procesos y sistemas de información, control y comunicaciones, que interactúan entre sí y con las personas, y en el que la información se crea, procesa, almacena y transmite.

Artículo 5. La Ciberseguridad es el estado que se alcanza mediante la aplicación de un sistema de medidas (organizativas, normativas, técnicas, educativas, políticas y diplomáticas), destinado a garantizar la protección y el uso legal del ciberespacio.

En la protección del ciberespacio se incluye la reducción de riesgos y vulnerabilidades, la creación de capacidades para detectar y gestionar eventos e incidentes y el fortalecimiento de la resiliencia.

Artículo 6. La situación o acontecimiento que puede causar daños a los bienes informáticos, sea una persona, un programa maligno o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema se denomina amenaza.

Artículo 7. Se denomina ataque al intento de acceso o acceso a un sistema o una red informática o terminal mediante la explotación de vulnerabilidades existentes en su seguridad.

Artículo 8. Se identifica como riesgo a la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático y cause un impacto negativo en la organización.

Artículo 9. La vulnerabilidad se identifica como el punto o aspecto del sistema que muestra debilidad al ser atacado o que puede ser dañada su seguridad; representa los aspectos falibles o atacables en el sistema informático y califica el nivel de riesgo de un sistema.

Artículo 10. El presente Decreto es de aplicación a los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales, los órganos del Poder Popular, el sistema empresarial y las unidades presupuestadas, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas y las personas naturales.

Artículo 11. Constituyen premisas de la seguridad de las TIC para la informatización de la sociedad y la defensa del Ciberespacio Nacional las siguientes:

a) Elevar la Ciberseguridad frente a las amenazas, los ataques y riesgos a los que se exponen las TIC;
b) garantizar que todos los activos de las TIC sean gestionados de acuerdo con los estándares y buenas prácticas en seguridad;
c) aumentar el nivel de atención a la seguridad de las TIC y garantizar que el personal vinculado a estas domine sus deberes y responsabilidades;
d) establecer las bases de un modelo integral de gestión de la seguridad que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales;
e) garantizar el cumplimiento de la legislación vigente en materia de seguridad de las TIC;
f) elevar la seguridad de las TIC mediante el desarrollo de la industria nacional de programas y aplicaciones informáticas;
g) potenciar la preparación de los profesionales de las TIC, la preservación de estos y el desarrollo integral del capital humano asociado a la actividad;
h) concebir la seguridad en todas las etapas de desarrollo e implantación de las TIC;
i) garantizar la seguridad y resiliencia de las redes y los sistemas de información empleados en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular;
j) posibilitar la integración de la investigación, desarrollo e innovación con la producción y comercialización de productos, tecnologías y servicios de seguridad; y
k) promover la cooperación e intercambio internacional en función de la Ciberseguridad y la gobernanza de Internet.

Artículo 12. La Seguridad de las TIC es el conjunto de medidas administrativas, organizativas, físicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las TIC; el empleo del término seguridad informática, tiene igual significado.

CAPÍTULO II
SISTEMA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Sección Primera
Estrategia y Planificación

Artículo 13. El Sistema de Seguridad de las TIC es el conjunto de medios humanos, técnicos y administrativos que, de manera interrelacionada garantiza diferentes grados de seguridad informática, en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

Artículo 14. El Sistema de Seguridad de las TIC se constituye a partir de los sistemas de seguridad existentes en las instituciones del país que posean o utilicen las TIC, en interés propio o de terceros, e incluye:

a) Operadores de redes de telecomunicaciones, en lo adelante operadores;
b) proveedores de servicios públicos y privados de acceso a Internet;
c) productor de equipos;
d) proveedor de servicios de red;
e) proveedores de servicios de las TIC;
f) usuarios de las TIC; y
g) entidades encargadas de la dirección, el control y la supervisión de la seguridad de las TIC, así como de las actividades relacionadas con la vigilancia tecnológica, la alerta temprana y la gestión de incidentes.

Artículo 15. Los mecanismos de seguridad comprenden la implementación de hardware o software diseñados o construidos para prevenir, detectar o responder a incidentes de seguridad.

Artículo 16. Se considera un incidente de seguridad cualquier evento que se produzca de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de la información y la comunicación o los procesos que con ellas se realizan.

Artículo 17. Cada entidad que haga uso de las TIC diseña, implanta, gestiona y mantiene actualizado un Sistema de Seguridad, a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos.

Artículo 18. A partir del Sistema de Seguridad diseñado, cada entidad elabora su Plan de Seguridad de las TIC.

Artículo 19. El diseño del Sistema de Seguridad de las TIC y la elaboración del Plan de Seguridad de cada entidad se realizan en correspondencia con las metodologías establecidas al respecto por el Ministerio de Comunicaciones.

Artículo 20. El Plan de Seguridad de las TIC de una organización es el documento que incluye, describe y aplica las políticas, medidas y procedimientos diseñados para esta a partir de los riesgos estimados, así como establece las responsabilidades de los diferentes actores que participan en su ejecución.

Artículo 21. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular y en aquellas entidades en que la cantidad, diversidad e importancia de las TIC lo requieran, según el análisis que para ello se realice, disponen de los cargos de especialistas de seguridad de las TIC que garanticen la atención de esta actividad.

Artículo 22. Los usuarios de las TIC asumen, en primera instancia, la responsabilidad de las consecuencias que se deriven de su utilización impropia.

Sección Segunda
Organización institucional, competencias y atribuciones

Artículo 23. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, el sistema empresarial y demás entidades, de acuerdo con su misión y funciones específicas, desarrollan las acciones que se establecen mediante el presente Decreto, en el marco del proceso de Informatización de la Sociedad Cubana.

Artículo 24. El Ministerio de Comunicaciones controla a todos los niveles de dirección de los organismos de la Administración Central del Estado y de las demás personas jurídicas, el cumplimiento de las normas de seguridad de las TIC, excepto aquellos que se determinen por ese propio Ministerio.

Artículo 25. El Ministerio de Comunicaciones, en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, establece las normas de seguridad de las TIC y se responsabiliza por la ejecución de las acciones siguientes:

a) Desarrollar y modernizar la infraestructura vinculada a la seguridad de las TIC para incrementar la efectividad en la protección del Ciberespacio Nacional mediante un enfoque sistémico, conceptual y organizativo;
b) impulsar la cooperación internacional y coordinar la participación en eventos que permitan adoptar normas globales para el desarrollo de la Seguridad de las TIC, así como defender la posición del país en materia de Ciberseguridad;
c) suscribir convenios que contribuyan a desarrollar soluciones de seguridad, ampliar el acceso y la transferencia del país a nuevas tecnologías, preparar el capital humano y contribuir al enfrentamiento de las amenazas en el plano internacional;
d) establecer el Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad y asegurar los procedimientos para su implementación en todos los niveles por parte de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, así como realizar el enfrentamiento y neutralización de estos sucesos atendiendo a lo que a cada organismo le corresponde;
e) establecer un sistema de trabajo entre las entidades especializadas en seguridad de las TIC que garantice el cumplimiento de sus funciones en el intercambio seguro de información relativa a vulnerabilidades e incidentes de Ciberseguridad, la colaboración y la coordinación entre sí, con el empleo de servicios seguros de voz, videoconferencia y datos;
f) organizar y potenciar de modo sostenible la investigación, el desarrollo, la innovación y el soporte tecnológico, en función de los sistemas para la Seguridad de las TIC;
g) perfeccionar y potenciar la supervisión, certificación, homologación y acreditación de las soluciones, servicios y la infraestructura tecnológica vinculados a la seguridad de las TIC;
h) asimilar y recibir transferencia tecnológica de las infraestructuras técnicas y organizacionales, de hardware y software, en centros de investigación para la seguridad, parques científicos-

tecnológicos, los sistemas operativos, los equipos de cómputo y los relacionados con la conectividad;

i) diseñar e implementar acciones de inspección, asistencia, consultoría y auditoría, de la seguridad de las TIC; así como para su control, en correspondencia con la categorización de los sistemas y actividades;
j) ejercer la fiscalización de la seguridad de las TIC;
k) fortalecer la estrategia de desarrollo del antivirus nacional;
l) garantizar el desarrollo de las actividades que los ministerios de las Fuerzas Armadas Revolucionarias y del Interior realizan para la supervisión y el control de los servicios de las TIC;
m) adquirir, asimilar y desarrollar equipamientos y soluciones para la supervisión y control de servicios y aplicaciones con impacto en la Seguridad Nacional;
n) instrumentar los mecanismos que organicen e incentiven la cooperación internacional en función del desarrollo de soluciones y tecnologías de seguridad en el territorio nacional;
o) garantizar el desarrollo de las actividades de supervisión y control de los servicios de las TIC;
p) perfeccionar de forma ordenada los sistemas y mecanismos de supervisión y control existentes sobre las TIC que utilizan el espectro radioeléctrico, así como garantizar la compatibilidad electromagnética y su uso seguro;
q) establecer los requerimientos básicos para las aplicaciones informáticas destinadas a la gestión de incidentes de Ciberseguridad;
r) organizar y controlar la protección de las principales redes informáticas y sistemas de trabajo que generan servicios de esta naturaleza, que constituyen Infraestructuras Críticas de las TIC, para dotarlas del nivel de seguridad en correspondencia con su categoría;
s) certificar la seguridad de las Infraestructuras Críticas de las TIC;
t) establecer e implementar el Sistema Nacional de Certificación de la Seguridad de las TIC y los laboratorios de certificación para evaluarla, en correspondencia con la categorización de los sistemas y actividades;
u) implementar y potenciar la Red de Gobierno con los requerimientos disponibles de máxima seguridad;
v) incrementar y fortalecer mecanismos de seguridad que permitan detectar y prevenir actividades nocivas en las redes informáticas de los operadores, así como en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular y demás entidades;
w) desarrollar e implementar proyectos propios de soluciones integrales, telemática, protección técnica integral y canales colaterales, programas y aplicaciones informáticas básicas, protección de activos digitales, licenciamiento y las soluciones para la Seguridad y Defensa Nacional y el Orden Interior, en correspondencia con la categorización de los sistemas y actividades;
x) desarrollar entrenamientos de Ciberseguridad en los ejercicios que se ejecuten para elevar la defensa del país en el Ciberespacio y comprobar la efectividad de los planes orientados a dar respuesta a incidentes de Seguridad de las TIC; e
y) incrementar la calidad de la gestión del capital humano especializado en la Seguridad de las TIC.

Artículo 26. El Ministerio de Comunicaciones, de conformidad con sus atribuciones y funciones específicas, es el responsable de las actividades siguientes:

a) Fortalecer la infraestructura de seguridad en las redes informáticas;
b) establecer y controlar la implementación de configuraciones básicas de seguridad orientadas al fortalecimiento de las aplicaciones y equipos que operan en el perímetro de las redes informáticas de las entidades;
c) adquirir y desarrollar equipamientos y programas informáticos especializados para el procesamiento y almacenamiento de las evidencias digitales relacionadas con incidentes de Ciberseguridad;
d) facilitar el hospedaje de los servicios de las entidades estatales y del sector no estatal en los centros de datos públicos para garantizar la racionalidad de las infraestructuras de seguridad y su despliegue y minimizar su diseminación;
e) perfeccionar el marco legal con la finalidad de sustentar la seguridad de las TIC en la informatización de la sociedad para establecer interoperabilidad, integridad, confidencialidad, disponibilidad y no repudio de la información;
f) establecer los mecanismos a emplear para la prevención y respuesta a incidentes de seguridad informática que involucren las TIC ubicadas en los hogares y las áreas públicas para el acceso al ciberespacio, por parte de las personas naturales y jurídicas; y
g) garantizar la recopilación de los incidentes de Ciberseguridad que se detecten.

Artículo 27. El Ministerio del Interior, de conjunto con el Ministerio de las Fuerzas Armadas Revolucionarias, de acuerdo con sus funciones específicas, es responsable de fortalecer los mecanismos de seguridad que permitan detectar y prevenir actividades enemigas y delictivas en las redes informáticas de los operadores, así como en las entidades.

Artículo 28. El Ministerio del Interior en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias y de Comunicaciones, realiza las acciones siguientes:

a) Organizar actividades para fortalecer la recopilación y el análisis nacional sobre Seguridad de las TIC; y
b) establecer la gestión de identidad como parte indispensable del proceso de registro y validación, en correspondencia con la legislación vigente.

Artículo 29. El Ministerio de las Fuerzas Armadas Revolucionarias, en coordinación con los ministerios del Interior y de Comunicaciones, mantiene actualizado el Procedimiento para la Compatibilización con la Defensa de los servicios, tecnologías e inversiones vinculadas a las TIC.

Sección Tercera
Del empleo seguro de las Tecnologías de la Información y la Comunicación

Artículo 30. La seguridad de la información oficial se rige por la legislación vigente que regula lo relativo a su protección, en cualquier soporte en el que se encuentre.

Artículo 31. Los requerimientos de seguridad para la proyección, diseño e instalación de locales tecnológicos en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, se establecen según lo dispuesto en la legislación vigente.

Artículo 32. Los ministerios del Interior y de Justicia, de acuerdo con sus funciones, son los encargados de regular y controlar la protección de la información correspondiente a las personas naturales y jurídicas y la privacidad de los datos personales.

Artículo 33. La entidad que por sus funciones posea o controle datos de las personas naturales o jurídicas es responsable de la protección de la información personal y la privacidad de los documentos y únicamente facilita a las autoridades competentes la supervisión y acceso a estos datos personales, en correspondencia con la legislación vigente.

Artículo 34. El que haga uso, procese, trasmita y almacene información de personas naturales y jurídicas, lo realiza bajo los principios de legalidad, propiedad y necesidad e indica, de forma explícita, a estas personas los objetivos y el alcance, y han de tener su consentimiento cuando se requiera.

Artículo 35. Las reglas para la recopilación y el uso de la información tienen carácter público y se divulgan de forma oportuna y precisa para garantizar el conocimiento por las personas naturales y jurídicas.

Artículo 36. Se consideran bienes informáticos a los elementos que componen el sistema informático que son protegidos para evitar que sufran algún tipo de daño, como resultado de la materialización de una amenaza.

Artículo 37. Los bienes informáticos de una entidad son utilizados en las funciones propias del trabajo, así como en tareas autorizadas por la dirección de esta.

Artículo 38. Todos los bienes informáticos de una entidad se identifican y controlan, para lo cual se conforma y mantiene actualizado su estado físico, incluidos sus componentes y las especificaciones técnicas de aquellos que pudieran ser sustituidos.

Artículo 39. Es un deber y un derecho de la dirección de la entidad el control y supervisión del correcto empleo de las TIC por parte de los usuarios y su uso no autorizado es sancionable según la legislación vigente.

Artículo 40. Los jefes a cada nivel garantizan que el personal vinculado a las TIC esté capacitado para su utilización, que conozca los deberes y derechos en relación con el Sistema de Seguridad Informática, así como que exista constancia del conocimiento y compromiso que asume este personal de forma individual.

Artículo 41. El Ministerio de Comunicaciones otorga una licencia de operación a las entidades que pueden brindar servicios de seguridad de las TIC a terceros.

Artículo 42. El acceso del personal a las facilidades de procesamiento y a los servicios que brindan las tecnologías requiere de autorización expresa y de un control estricto de su uso por la dirección de cada entidad, las que establecen los requerimientos específicos para garantizar la seguridad, a partir de los riesgos que esto pueda introducir.

Artículo 43. La unidad organizativa que corresponda en cada entidad, de acuerdo con su estructura, exige a los usuarios de las TIC el cumplimiento de la información inmediata de cualquier incidente de seguridad, debilidad o amenaza a los sistemas y servicios con que opera.

Artículo 44. Se denomina Barrera de Protección al dispositivo físico o lógico utilizado para proteger un sistema informático o red de telecomunicaciones y obstaculizar el acceso a estos o entre sus componentes, ya sea de forma directa o remota.

Artículo 45. La dirección de cada entidad determina aquellos equipamientos de las TIC que por las funciones a las que se destinan, la información que contengan y las condiciones de los locales en que se encuentran ubicados, requieren la aplicación específica de medidas especiales de protección física y asegura una barrera de protección a estos medios que impida su empleo en la comisión de hechos intencionales que violen lo establecido o en actividades delictivas.

Artículo 46. El Ministerio de Comunicaciones ejecuta periódicamente las acciones de control a la seguridad de las TIC siguientes:

a) Realizar diagnósticos integrales en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, tanto tecnológicos como organizativos, que permitan evaluar el estado de la seguridad de las TIC e implementar acciones correctivas para su solución;
b) evaluar sistemáticamente las condiciones de seguridad de las aplicaciones informáticas, tanto en su codificación y despliegue como en la ejecución y trazabilidad de las operaciones realizadas; y
c) diseñar y establecer los mecanismos de comprobación de la Seguridad de las TIC que se utilizan por las personas naturales y jurídicas para acceder al ciberespacio.

Artículo 47. En cada entidad se implementan los controles y procedimientos que los protegen contra programas malignos, con el fin de mitigar sus efectos nocivos e impedir su generalización; para la protección contra virus informático se utilizan los programas antivirus de producción nacional y otros autorizados para su uso en el país, con un soporte establecido que permita su actualización.

Artículo 48. El Virus Informático es el programa capaz de reproducirse a sí mismo sin que el usuario esté consciente de ello; se adiciona a programas de aplicación, así como a componentes ejecutables del sistema, de forma tal que pueda tomar el control de este durante la ejecución del programa infectado.

Artículo 49. Queda prohibido el envío de mensajes masivos que:

a) Sean no deseados (Spam); que se entiende por toda información de voz o datos transmitida o enviada de forma masiva, indiscriminada y repetitivamente por medio de las redes de telecomunicaciones, sin el previo consentimiento de sus destinatarios.
b) no contenga, sea falso u oculto el asunto y la dirección o ubicación física o electrónica, número telefónico, identidad u otro medio de identificación del emisor e impidan a los destinatarios o receptores notificar su voluntad de no recibir más mensajes o no incluyan mecanismos que permitan al receptor manifestar su voluntad de no recibirlos;
c) afecten el uso seguro y la calidad de las redes de telecomunicaciones de Cuba o de otros países o de los servicios que se prestan a través de estas; y
d) posean un contenido que transgreda lo establecido en la legislación vigente cubana o los tratados, convenios o cualquier otro instrumento jurídico de carácter internacional de los que la República de Cuba es Estado parte.

Artículo 50. Los mensajes que contengan las características referidas en el Artículo anterior se consideran mensajes masivos dañinos.

Artículo 51. Corresponde a los operadores y proveedores:

a) Bloquear el envío, recepción o transmisión de los mensajes masivos dañinos que se cursan por sus redes y utilizan sus servicios;
b) suspender temporalmente por hasta un mes las comunicaciones entre sus redes y las que se establecen con las redes de operadores o proveedores extranjeros que no adopten las medidas necesarias para impedir el tráfico de mensajes masivos dañinos, lo que se notifica antes de las 72 horas posteriores a su suspensión y, en igual término, dar cuenta al Ministerio de Comunicaciones; y
c) suspender temporalmente por hasta un mes el servicio prestado a los usuarios responsables del envío de mensajes masivos dañinos, lo que se notifica antes de las 72 horas posteriores a su suspensión y, en igual término, da cuenta al Ministerio de Comunicaciones, a los órganos del Ministerio del Interior o de la Fiscalía General de la República.

Artículo 52. En los contratos suscritos por los operadores y proveedores entre sí y con sus usuarios, se incluye una cláusula sobre la responsabilidad derivada del envío de mensajes masivos dañinos a través de las redes de telecomunicaciones con utilización de las TIC o de los equipos terminales de telecomunicaciones que son objeto de control por el Ministerio de Comunicaciones y, ante su incumplimiento, se le aplican las medidas previstas en la legislación vigente.

Artículo 53. Es responsable del envío de mensajes masivos dañinos toda persona natural o jurídica que:

a) directamente los envíe;
b) los genere a través de los equipos de telecomunicaciones de otras personas;
c) los transporte o intermedie en su difusión o trasmisión o haya incidido en su contenido, si mediante sus medios técnicos lo hubiese conocido y no evita su transportación, difusión, trasmisión, envío y reenvío; y
d) cree, venda, preste, intercambie o realice cualquier tipo de recolección o transferencia de listas de direcciones de correo electrónico, números telefónicos u otro medio de identificación del emisor que haya sido realizada sin la autorización o consentimiento de su titular o del operador o proveedor de los servicios y sean conformadas para el envío de mensajes masivos dañinos.

Sección Cuarta
De la Seguridad de las Operaciones

Artículo 54. La seguridad de las operaciones realizadas sobre las TIC es garantizada por la protección desplegada de seguridad de la red por niveles para evitar interferencias, daños o accesos no autorizados, fugas de datos, robos o falsificación.

Artículo 55. Se denomina traza al registro cronológico de las acciones que se realizan en un sistema, el acceso a este y los procesos y ficheros que han intervenido.

Artículo 56. Los proveedores de servicio de acceso a Internet, para garantizar la seguridad de sus operaciones, cumplen con los deberes siguientes:

a) elaborar procedimientos de operación y gestión de seguridad internos;
b) determinar las personas responsables de la seguridad de la red y los sistemas que soporta, así como implementar mecanismos efectivos de control y supervisión sobre la actividad que realizan;
c) adoptar medidas técnicas y organizativas para prevenir la contaminación con programas malignos, ataques e intrusiones en la red, así como otras acciones que pongan en peligro la seguridad de las TIC;
d) elaborar planes de respuesta a incidentes de seguridad que establezcan medidas para su prevención y, en caso de ocurrencia, aseguren la actuación bajo el principio de la racionalidad y en correspondencia con lo establecido a esos efectos;
e) establecer el registro y la trazabilidad de las operaciones realizadas, así como el control de los eventos e incidentes, en correspondencia con las regulaciones vigentes;
f) aplicar mecanismos que aseguren la preservación de evidencias digitales, la clasificación de los datos sensibles y el cifrado; y
g) establecer la obligatoriedad de las personas naturales y jurídicas de preservar las trazas de los servicios utilizados para acceder al ciberespacio.

Artículo 57. Los responsables de la instalación y operación del equipamiento perimetral de las redes informáticas y los productos especializados de seguridad, cumplen con la legislación vigente relativa a los requerimientos de la Seguridad y Defensa Nacional; los requisitos establecidos en las normas nacionales son evaluados por la entidad autorizada por el Ministerio de Comunicaciones a través de la implementación de las medidas siguientes:

a) Establecer un catálogo de equipos y servicios especializados de seguridad considerados como críticos; y
b) promover el reconocimiento recíproco, entre las entidades especializadas en seguridad de las TIC, de certificaciones de seguridad y los resultados de controles, inspecciones y auditorías, para evitar la duplicación de esfuerzos.

Artículo 58. Al determinar las responsabilidades asignadas al personal que labora en las áreas relacionadas con la seguridad informática, se tiene en cuenta el principio de separación de funciones y se especifican las tareas que no pueden ser ejecutadas por una misma persona, a fin de reducir oportunidades de modificación no autorizada, o uso inadecuado de los sistemas de las TIC.

Artículo 59. El jefe de la entidad es el responsable de la introducción de los servicios de las TIC, actualizaciones y nuevas versiones, en correspondencia con el sistema de seguridad establecido y los resultados de las pruebas realizadas, para determinar si cumple los criterios de seguridad apropiados.

Artículo 60. Los sistemas informáticos en que es posible el acceso por múltiples usuarios disponen de un identificador de usuario personal y único; y las personas a las que se le asignen identificadores de usuarios responden por las acciones que con ellos se realicen; en caso del cese de la relación laboral u otras causas que se determine por la dirección de la entidad se procede a eliminar el identificador del usuario; en todos los casos se preservan las trazas de uso de las credenciales de acceso, por un tiempo no menor de un año.

Artículo 61. La entidad establece un procedimiento para la asignación de los identificadores de usuarios en los sistemas, que incluye en el caso de los nuevos la solicitud previa al jefe inmediato superior y su posterior notificación al interesado.

Artículo 62. La entidad implementa un sistema fiable de respaldo de la información esencial para su funcionamiento, que permita su recuperación después de un ataque informático, desastre o fallo de los medios, para ello ejecuta los procedimientos que aseguren la obtención sistemática de las copias que se requieran.

Artículo 63. La información de respaldo, conjuntamente con informes precisos y completos de sus copias y los procedimientos de recuperación documentados, se almacenan en otra ubicación, que le permita no afectarse en caso de desastre en la ubicación principal.

Artículo 64. La información de respaldo requiere una protección física y ambiental consecuente con las normas aplicadas en la ubicación principal; los controles realizados a los medios en la ubicación

principal se extienden a los medios de respaldo.

Artículo 65. Los medios de respaldo se prueban regularmente y se verifica el estado de actualización de la información almacenada, con el fin de asegurar la confiabilidad en ellos para un uso de emergencia, cuando sea necesaria la ejecución de un proceso de recuperación.

Artículo 66. El jefe de la entidad establece la utilización obligatoria del antivirus nacional y su despliegue en la red privada.

Artículo 67. El Ministerio de Comunicaciones aprueba la utilización de un antivirus extranjero para su uso en el país, cuando este se justifique, y promueve el fortalecimiento del motor del antivirus nacional a partir de la asimilación de otros motores de antivirus.

Artículo 68. El Ministerio de Comunicaciones promueve el desarrollo y la comercialización de los servicios de instalación y actualización del antivirus nacional y las licencias para su uso por las personas naturales y jurídicas.

Artículo 69. La entidad puede adquirir la infraestructura y el equipamiento especializado necesario para la captura de muestras de programas malignos que incorpora a la base de datos del antivirus nacional.

Artículo 70. El Ministerio de Comunicaciones, en coordinación con los Ministerios de Educación y Educación Superior, diseña e implementa proyectos de investigación y desarrollo sobre la seguridad de las TIC en colaboración con centros académicos y de investigación del país, dentro de los que se incluyen los de los ministerios de las Fuerzas Armadas Revolucionarias y del Interior.

Sección Quinta
De la seguridad en el empleo de las redes

Artículo 71. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, de conjunto con los ministerios de Economía y Planificación y el de Finanzas y Precios, evalúan el respaldo financiero para incrementar la Seguridad de las TIC en las redes informáticas, de manera estable y sostenida, a partir de considerar la importancia de la información y los servicios que sustentan, el que se define en el Plan anual de la Economía.

Artículo 72. En todas las redes de datos se habilitan las opciones de seguridad con que cuentan los sistemas operativos, de forma tal que garanticen la protección de los servidores y las terminales, el acceso a la información solamente por personal autorizado y los elementos que permitan la supervisión y auditoría de los principales eventos por un tiempo no menor de un año.

Artículo 73. El jefe del área o de la unidad organizativa que atiende las TIC responde por la implementación y ejecución de los procedimientos y normas que garanticen el empleo seguro de las TIC de forma general y la protección de la seguridad de la red por niveles para evitar interferencias,

daños o accesos no autorizados, fugas de datos, robos o falsificación de forma particular; para lograr este objetivo tiene las responsabilidades siguientes:

a) Determinar las personas responsables de la seguridad de la red y los sistemas que soporta, así como implementar mecanismos efectivos de control y supervisión sobre la actividad que realizan, así como aquellos que permitan filtrar o depurar la información que se intercambie.
b) adoptar las medidas técnicas y organizativas para prevenir la contaminación con programas malignos, ataques e intrusiones en la red, así como otras acciones que pongan en peligro la seguridad de las TIC;
c) elaborar planes de respuesta a incidentes de seguridad que establezcan medidas para su prevención y, en caso de ocurrencia, aseguren la actuación bajo el principio de la racionalidad y en correspondencia con lo establecido a esos efectos; y
d) aplicar mecanismos que aseguren la preservación de evidencias digitales, la clasificación de los datos sensibles, el cifrado y las trazas de los servicios utilizados para acceder al ciberespacio por parte de las personas naturales y jurídicas.

Artículo 74. El jefe del área o de la unidad organizativa que atiende las TIC asegura la instalación de las herramientas de seguridad autorizadas por el Ministerio de Comunicaciones para la fiscalización y la supervisión del empleo de las redes de datos y de los servicios implementados.

Artículo 75. La arquitectura y la configuración de los diferentes componentes de seguridad de una red de datos y la implementación de sus servicios están en correspondencia con el Plan de Seguridad de las TIC, y en ningún caso son el resultado de la iniciativa de una persona, con independencia de la preparación que posea.

Artículo 76. Toda red de datos requiere para su operación de la presencia de, al menos, una persona encargada de su administración.

Artículo 77. La gestión de administración de las redes de datos implica la concesión de privilegios requeridos para la tarea que cumple, los que se realizan directamente desde el puesto de trabajo que ocupe; se prohíbe la administración remota de estas redes de datos a través de redes públicas sin mecanismos criptográficos autorizados por los organismos competentes.

Artículo 78. Los usuarios que han recibido la autorización para el empleo de los servicios que brindan las redes son responsables de su propia conducta; para ello conocen y cumplen los planes de seguridad de las TIC.

Artículo 79. Los jefes de las redes de datos o equipos que prevean conexiones desde o hacia el exterior de una entidad, instalan los medios técnicos que aseguren una barrera de protección entre las TIC de la entidad de que se trate y la red externa, con los mecanismos de seguridad que sea necesario implementar.

Artículo 80. La dirección de la entidad instrumenta la ejecución de procedimientos periódicos de

verificación de la seguridad de sus redes de datos, con la finalidad de detectar posibles vulnerabilidades, incluido para ello, cuando sea procedente y debido a la sensibilidad de estas acciones, la comprobación de forma remota por entidades autorizadas oficialmente.

Artículo 81. El jefe del área o de la unidad organizativa que atiende las TIC que coloque información en servidores para su acceso público establece las medidas y procedimientos que garanticen su integridad y disponibilidad, así como la correspondencia de su contenido con sus intereses y los del país.

Artículo 82. Cuando por necesidades de conectividad u otros intereses, la entidad requiere hospedar un sitio en servidores ubicados en un país extranjero, esto se realiza como espejo o réplica del sitio principal en servidores ubicados en Cuba y se establecen las medidas requeridas para garantizar su seguridad, en particular durante el proceso de actualización de la información.

Artículo 83. Los servidores de redes de una entidad destinados a facilitar accesos hacia o desde el exterior y los de uso interno deben estar instalados en zonas diferentes de la red, de forma tal que evite la conexión entre estos.

Artículo 84. La dirección de la entidad autoriza el acceso de su personal a Internet y los servicios asociados a este, en correspondencia con sus intereses y necesidades, según las normas particulares establecidas para estos servicios, y documenta esta autorización de manera que pueda ser objeto de comprobación.

Artículo 85. Las redes proveedoras de servicios han de tener las medidas que se requieran para impedir la sobrecarga de los canales de comunicaciones, restringir el envío o recepción de grandes volúmenes de información y la generación de mensajes a múltiples destinatarios.

Artículo 86. La dirección de la entidad implementa controles dirigidos a impedir e interrumpir la generación de cartas en cadena y el envío de mensajes de correo de forma masiva a través de las redes.

Artículo 87. La dirección de una entidad con redes de datos destinadas a proveer servicios a otras personas naturales o jurídicas mediante conexiones remotas, cumple los requisitos siguientes:

a) Establecer las medidas y procedimientos de seguridad de las TIC que garanticen la protección de los servicios a brindar y los intereses de seguridad de los que los reciben;
b) implementar los mecanismos y procedimientos que aseguren la identificación del origen de las conexiones, incluidas las conmutadas, así como su registro y conservación por un tiempo no menor de un año;
c) informar a los clientes de estos servicios los requerimientos de seguridad informática que tienen que cumplir, en correspondencia con el Plan de Seguridad de las TIC establecido en la red que los brinda; y
d) facilitar el acceso de las autoridades competentes a los registros de las conexiones y cooperar

en la investigación de violaciones de las normas establecidas y de incidentes de seguridad.

Artículo 88. La entidad autorizada es la única que puede explorar o monitorear las redes públicas de transmisión de datos, en busca de vulnerabilidades o información sobre sus usuarios.

Artículo 89. Los productores de equipos, los proveedores de servicios de red y de programas, aplicaciones y servicios informáticos, tanto nacionales como extranjeros, responden por la implementación de los requerimientos que garanticen el empleo seguro de los equipos y servicios que suministran.

Artículo 90. Las personas naturales o jurídicas, nacionales y extranjeras, usuarios de las TIC, responden por la utilización adecuada de los servicios y productos que emplean.

Artículo 91. Los cables de alimentación o de comunicaciones de las redes que transporten datos o apoyen los servicios de información se protegen contra la intercepción o el daño; el tendido de los cables de alimentación eléctrica se realiza de acuerdo con las normas establecidas a esos efectos, separados adecuadamente de los de comunicaciones para evitar posibles interferencias.

Artículo 92. El jefe de cada entidad garantiza que la instalación y operación del equipamiento perimetral de las redes informáticas y los productos especializados de seguridad se realicen en correspondencia con los requerimientos de la seguridad y defensa nacional, y que cumplan los requisitos establecidos en estándares nacionales elaborados a esos efectos y que sean aprobados por una entidad autorizada.

Artículo 93. La entidad aprobada por la autoridad competente para la creación de productos o soluciones informáticas, que implementan herramientas criptográficas, se rige por la legislación vigente.

Sección Sexta
Gestión de incidentes de seguridad

Artículo 94. La gestión de incidentes es el proceso que se realiza con el objetivo de prevenir, detectar y enfrentar los de Ciberseguridad y comprende las acciones que se realizan antes, durante y después de su ocurrencia.

Artículo 95. El jefe de la entidad dispone de las medidas y procedimientos que garanticen la continuidad, el restablecimiento y la recuperación de los procesos informáticos, como respuesta a incidentes de Ciberseguridad y en correspondencia con el Modelo de Actuación Nacional.

Artículo 96. Las medidas y procedimientos de recuperación son definidos a partir de la identificación de los posibles eventos que puedan causar la interrupción o afectación de los procesos informáticos e incluyen las acciones de respuesta, la determinación de los responsables de su cumplimiento y los recursos necesarios en cada caso.

Artículo 97. Los procedimientos para la gestión de incidentes y violaciones de Seguridad de las TIC

especifican la obligación de informar su ocurrencia y los pasos a seguir para garantizar una correcta evaluación de lo sucedido, a quién, cómo y cuándo se reporta la respuesta, los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial.

Artículo 98. El Ministerio de Comunicaciones potencia la incorporación del Equipo de Respuesta a Incidentes Computacionales de Cuba a los mecanismos regionales e internacionales que agrupan a ese tipo de organizaciones.

CAPÍTULO III
INFRAESTRUCTURAS CRÍTICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 99. El Ministerio de Comunicaciones, en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, es el responsable de elaborar y actualizar el Catálogo Nacional de Infraestructuras Críticas de las TIC y el Plan Nacional para la Protección de las Infraestructuras Críticas de las TIC.

Artículo 100. Los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, según corresponda, establecen y organizan sus Infraestructuras Críticas de las TIC relacionadas con la Seguridad y Defensa Nacional.

Artículo 101. El Ministerio de Comunicaciones, en coordinación con los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, organiza el trabajo de protección de las Infraestructuras Críticas de las TIC para dotarlas de la seguridad requerida y controla su correcto despliegue por parte de las entidades especializadas, en correspondencia con el nivel de seguridad requerido.

Artículo 102. El Sistema Nacional de Protección de las Infraestructuras Críticas de las TIC es el conjunto de medidas, previsiones y acciones que se generan, adoptan y ejecutan de forma integral y permanente, con el objetivo de preparar, organizar, ejercer y dirigir la protección de las infraestructuras críticas de las TIC, para lo cual se establecen las políticas, estructuras organizativas, normas y recursos orientados a ese fin, así como se dispone un flujo de información que abarque a todos sus integrantes.

Artículo 103. El Plan Nacional de Protección a las Infraestructuras Críticas de las TIC tiene como objetivo establecer los criterios y las directrices precisas para movilizar las capacidades operativas de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en coordinación con los operadores de las infraestructuras críticas y articular las medidas preventivas necesarias para asegurar su protección permanente, actualizada y homogénea.

Artículo 104. El Ministerio de Comunicaciones, de conjunto con los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, coordina las actividades de prevención, evaluación, aviso, investigación y respuesta a las acciones que afecten el funcionamiento de las Infraestructuras Críticas de las TIC.

Artículo 105. El jefe de la entidad responde por la garantía de la confidencialidad de los datos sobre Infraestructuras Críticas de las TIC a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada; además garantiza que el personal vinculado a las infraestructuras críticas de las TIC esté capacitado para su utilización, posean compromiso político, ético y de responsabilidad social y material; así como que conozcan sus deberes y derechos específicos en relación con estas.

Artículo 106. Los sistemas, las comunicaciones y la información referida a la protección de las Infraestructuras Críticas de las TIC tienen las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

CAPÍTULO IV
DE LA INSPECCIÓN Y LOS INCUMPLIMIENTOS EN LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 107. El Ministerio de Comunicaciones tiene como función estatal la ejecución de las inspecciones en materia de seguridad de las TIC, la que se realiza por sus inspectores y entidades autorizadas por este.

Artículo 108. El jefe de la entidad faculta a especialistas debidamente preparados para realizar controles en materia de seguridad informática a otras entidades atendidas, adscritas, subordinadas y patrocinadas.

Artículo 109. Las entidades y las personas naturales que incumplan lo dispuesto en el presente Decreto y en las disposiciones legales vigentes, están sujetas a la aplicación de las medidas siguientes:

a) Notificación preventiva;
b) invalidación temporal, parcial o cancelación de las autorizaciones administrativas concedidas por el Ministerio de Comunicaciones;
c) suspensión temporal, parcial o la cancelación de los servicios de informática y comunicaciones que hayan suscrito con empresas debidamente reconocidas y autorizadas por el Estado cubano;
d) decomiso de los medios, instrumentos, equipamientos y otros, utilizados para cometer la infracción; y
e) la aplicación de otras medidas que correspondan, de conformidad con lo legalmente establecido.

Artículo 110. Las entidades y las personas naturales sujetas a la aplicación de las medidas descritas en el Artículo anterior tienen derecho a interponer recurso en la vía administrativa, según lo dispuesto en el Decreto-Ley No. 370, del 17 de diciembre del 2018, “Sobre la Informatización de la Sociedad en Cuba”.

CAPÍTULO V
CAPACITACIÓN Y DIVULGACIÓN SOBRE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 111. El Ministerio de Finanzas y Precios, en coordinación con el Ministerio de Economía y Planificación, define las fuentes de financiamiento, orientadas a la adquisición de tecnologías de seguridad y a la preparación técnica de los especialistas en seguridad de las TIC.

Artículo 112. Los ministerios de Educación y de Educación Superior crean programas educativos y estrategias de trabajo que contribuyan a incrementar la conciencia en la sociedad acerca de la importancia de preservar la información personal.

Artículo 113. El Ministerio de Comunicaciones, en coordinación con el Instituto Cubano de Radio y Televisión, el Ministerio de Cultura y otras instituciones, promueve el uso de los medios de difusión para la trasmisión de mensajes educativos relacionados con la seguridad de las TIC.

Artículo 114. Cada entidad es responsable por la superación de los especialistas en las diferentes áreas del conocimiento, relacionadas con la seguridad de las TIC de acuerdo con su nivel de especialización.

Artículo 115. El jefe de la entidad implementa acciones que contribuyan y propicien la permanencia y el tratamiento diferenciado del personal que cumple funciones como especialistas de seguridad informática, en correspondencia con su categorización.

Artículo 116. La preparación en las materias objeto del presente Decreto de los cuadros, funcionarios y especialistas se desarrolla mediante acciones de carácter educativo-preventivas que estén relacionadas con los planes de estudios de las escuelas o centros docentes que correspondan.

Artículo 117. Los ministerios de Educación y Educación Superior insertan en los planes de estudio los temas referentes a la Seguridad de las TIC en todos los niveles de enseñanza, e implementan planes de estudios para los especialistas en seguridad de las TIC, actualizados por normas internacionales, así como fomentan los intercambios académicos e investigativos con universidades y centros de investigaciones nacionales e internacionales con alta preparación en la temática.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas lo establecido en el presente Decreto, de conformidad con sus estructuras.

DISPOSICIONES FINALES

PRIMERA: Los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización y establecen las coordinaciones que resulten necesarias relativas a la aplicación del presente Decreto.

SEGUNDA: El Ministerio de Trabajo y Seguridad Social actualiza los calificadores y jerarquiza los cargos, a partir de las competencias requeridas para el perfil ocupacional del especialista en seguridad de las TIC.

TERCERA: El glosario de términos y definiciones anexo forma parte del contenido del presente Decreto.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, a los 31 días del mes mayo de 2019.

MIGUEL DÍAZ-CANEL BERMÚDEZ
Presidente de los consejos de Estado y de Ministros

JORGE LUIS PERDOMO DI-LELLA
Ministro de Comunicaciones

ANEXO
GLOSARIO DE TÉRMINOS Y DEFINICIONES

1) Entidad: Todos los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro y las organizaciones políticas, sociales y de masas.

2) Infraestructuras críticas de las Tecnologías de la Información y la Comunicación: son aquellas que soportan los componentes, procesos y servicios esenciales que garantizan las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública.

3) Órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular: Todos los órganos superiores del Estado y del Gobierno, los órganos locales del Poder Popular, los organismos de la Administración Central del Estado, las organizaciones superiores de dirección empresarial que

incluye a la Empresa de Telecomunicaciones de Cuba S.A.

DECRETO No. 359/2019

MIGUEL DÍAZ-CANEL BERMÚDEZ, Presidente de los consejos de Estado y de Ministros de la República de Cuba.

HAGO SABER: Que el Consejo de Ministros ha considerado lo siguiente:

POR CUANTO: El Decreto-Ley No. 370 “Sobre la Informatización de la Sociedad en Cuba”, del 17 de diciembre del 2018, en su Disposición Final Primera encarga al Consejo de Ministros dictar disposiciones complementarias sobre la Industria de Programas y Aplicaciones Informáticas.

POR CUANTO: El referido Decreto-Ley No. 370, establece las regulaciones generales aplicables a la determinación del alcance de la Industria Cubana de Programas y Aplicaciones Informáticas para promover, perfeccionar e incrementar la producción nacional y las exportaciones de los productos de la industria y a la sustitución de importaciones, acciones que requieren ser implementadas mediante las normas complementarias que resulten necesarias.

POR TANTO: El Consejo de Ministros, en el ejercicio de las atribuciones que le están conferidas en el Artículo 137, incisos ñ) y o), de la Constitución de la República de Cuba, decreta lo siguiente:

DECRETO NO. 359

SOBRE EL DESARROLLO DE LA INDUSTRIA CUBANA DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

CAPÍTULO I
OBJETO, OBJETIVOS Y ÁMBITO DE APLICACIÓN

Artículo 1. El Estado promueve el desarrollo y utilización de la Industria Cubana de Programas y Aplicaciones Informáticas, en lo adelante la Industria, con el objetivo de contribuir a respaldar las prioridades de la informatización en beneficio de la economía, la sociedad y la Seguridad y Defensa Nacional, para alcanzar un crecimiento sustancial de su ejecución y servicios asociados.

Artículo 2. El presente Decreto tiene como objeto establecer el marco legal reglamentario que ordene y garantice el derecho al acceso y participación de las personas en el desarrollo de la Industria cubana de programas y aplicaciones informáticas, en correspondencia con lo establecido en la Constitución, las leyes y las restantes disposiciones legales relacionadas con el tema, así como los acuerdos internacionales en esta materia de los que la República de Cuba es Estado parte.

Artículo 3. Resulta de aplicación este Decreto a las relaciones jurídicas que se establecen entre los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, el sistema empresarial y las formas de propiedad y gestión no estatal cuyo objeto social o actividad comprenda el desarrollo de programas y aplicaciones informáticas y la prestación de servicios informáticos asociados a esta industria.

Artículo 4. Los objetivos del presente Decreto son los siguientes:

a) Promover la empresa estatal socialista, como actor principal en esta industria y, de conjunto con las formas de propiedad y gestión no estatal, contribuir a la informatización de la sociedad, la sustitución de importaciones y a las exportaciones;
b) preservar y desarrollar el capital humano asociado a la actividad y estimular su vínculo con las prioridades de informatización de la sociedad;
c) fortalecer la capacidad de la Industria para contribuir a la soberanía tecnológica, la ciberseguridad, la sostenibilidad y crecimiento económico del país y al bienestar social; e
d) impulsar la integración de la investigación, el desarrollo y la innovación con la producción y comercialización de los productos y servicios informáticos.

Artículo 5. La Industria, comprende a las entidades y al trabajador por cuenta propia que se relacionan con el desarrollo de programas y aplicaciones informáticas y la prestación de servicios informáticos, que estén inscritos en el control administrativo del Ministerio de Comunicaciones.

Artículo 6. Las entidades y el trabajador por cuenta propia solicitan al Ministerio de Comunicaciones su incorporación a la Industria, según los requisitos que este establezca.

Artículo 7. Los principios sobre los que se sustenta la Industria cubana de programas y aplicaciones informáticas son:

a) La satisfacción de las exigencias de la informatización de la sociedad cubana;
b) la contribución a la soberanía tecnológica, la ciberseguridad, la sostenibilidad y al crecimiento económico del país;
c) la atención al capital humano asociado a la actividad;
d) la integración de la investigación, el desarrollo y la innovación para la producción y comercialización de productos y servicios;
e) la coherencia en el desarrollo de la Industria y el aprovechamiento de los diferentes actores del modelo económico cubano; y
f) la exportación de productos y servicios, con participación de todas las formas de propiedad y gestión no estatal existentes en el modelo económico cubano.

CAPÍTULO II
ORGANIZACIÓN INSTITUCIONAL Y COMPETENCIAS

Artículo 8. El Ministerio de Comunicaciones es el organismo encargado de proponer, coordinar y controlar el cumplimiento de las políticas y estrategias asociadas al proceso de organización y desarrollo de la Industria y en el ejercicio de sus funciones específicas cumple las acciones siguientes:

a) Propone, coordina, controla y emite directrices asociadas al proceso de organización y desarrollo de la Industria para garantizar el cumplimiento de las normas jurídicas, procedimientos y metodologías y el funcionamiento de los procesos que aseguren su sinergia;
b) inscribe en el control administrativo a las entidades y al trabajador por cuenta propia que conforman la Industria y establece los requisitos que deban cumplir y lo publica en el sitio web;
c) atiende de manera priorizada y diferenciada los proyectos del programa nacional de informatización;
d) promueve y coordina el desarrollo de programas, aplicaciones y servicios informáticos, en correspondencia con las prioridades de informatización del país, así como la capacitación permanente del capital humano de la Industria y el acceso a la información por directivos y funcionarios vinculados a estas actividades, en función de contribuir a la efectividad en el desempeño de su labor;
e) evalúa y controla los planes de acción que desarrollan las entidades y el trabajador por cuenta propia en función del proceso de organización de la Industria, así como asegura el empleo ordenado de las capacidades humanas y tecnológicas del país;
f) diseña e implementa una estrategia de comunicación sobre la Industria y sus resultados, que contribuya al proceso de informatización de la sociedad, así como evalúa sistemáticamente su efectividad;
g) constituye grupos de expertos con el fin de contribuir a la formulación de políticas y estrategias y a la evaluación de su impacto, para proyectar e implementar soluciones informáticas ante los retos que impone el desarrollo y aplicación de las nuevas tecnologías en procesos priorizados de la nación;
h) coordina los esfuerzos nacionales de investigación, desarrollo e innovación en el terreno de las aplicaciones, programas informáticos y servicios asociados; supervisa la protección de sus resultados, en especial los que tengan mayor utilización en los frentes estratégicos del país;
i) impulsa la cooperación internacional y la realización de eventos con la finalidad de lograr una mayor integración de la Industria, ampliar las capacidades del país y asimilar modelos de gestión para el desarrollo de los programas y aplicaciones informáticas y servicios asociados, con el fin de contribuir a la informatización de la sociedad, la prevención y el enfrentamiento a los eventos nocivos en el ciberespacio;
j) aprueba las normas jurídicas asociadas al desarrollo de esta Industria; controla y fiscaliza su cumplimiento; e
k) identifica los principales proyectos informáticos, con el fin de crear las capacidades de desarrollo de la Industria que permitan su impulso.

Artículo 9. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, de acuerdo con su misión y funciones

específicas aprobadas, desarrollan las acciones que se establecen mediante el presente Decreto, en el marco del proceso de Informatización de la Sociedad Cubana.

CAPÍTULO III
DE LAS ACCIONES PARA FORTALECER LA INDUSTRIA CUBANA DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

Artículo 10. Corresponde al Ministerio de Comunicaciones, en el marco del proceso de organización y desarrollo de la Industria Cubana de Programas y Aplicaciones Informáticas y de conformidad con sus funciones específicas aprobadas, coordinar con los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular competentes, la implementación de las acciones y medidas básicas para de forma integral garantizar el desarrollo de esta Industria.

Artículo 11. En el marco del proceso de organización y desarrollo de la Industria, los organismos de la Administración Central del Estado y el Banco Central de Cuba mencionados a continuación, realizan las acciones y medidas siguientes:

Ministerio del Comercio Exterior y la Inversión Extranjera:

1) Promueve la inversión extranjera y otras formas de asociación, para contribuir al crecimiento de las exportaciones y al progreso de la Industria, en función del interés nacional y la necesidad de potenciar el capital humano;
2) establece e implementa normas que regulen la importación de productos y servicios informáticos en correspondencia con las necesidades del país; e
3) implementa programas de exportación de servicios profesionales especializados en tecnología de la información y la comunicación, en lo adelante TIC e intensifica la cooperación internacional para el intercambio de expertos y la transferencia de tecnologías.

Ministerio de Comunicaciones:

1) Identifica, evalúa y propone políticas y estrategias para la organización de la Industria de programas y aplicaciones informáticas, con el objetivo de fomentar el desarrollo de la empresa estatal informática, de conjunto con las formas de propiedad y gestión no estatal para contribuir al desarrollo de la informatización de la sociedad y a sus exportaciones;
2) adopta un modelo organizativo que garantice el desarrollo y la sostenibilidad económica de la Industria;
3) incrementa la participación de la Industria en los proyectos priorizados por el país y favorece el desarrollo de los programas y aplicaciones informáticas vinculadas a los servicios;
4) favorece la diversificación de entidades especializadas que brinden servicios asociados a las TIC;
5) potencia el desarrollo y alcance de la autoridad nacional de calidad de programas y aplicaciones informáticas y fomenta la creación de empresas estatales que contribuyan de

forma intensiva y efectiva a la evaluación, normalización, certificación de la calidad de los programas y aplicaciones informáticas y servicios asociados a las TIC desarrollados en el país, así como promueve la certificación y acreditación de entidades, procesos, especialistas, soluciones y equipamiento informáticos;

6) colabora en la elaboración de los programas de formación y capacitación de especialistas;
7) promueve el desarrollo de parques científicos-tecnológicos como parte integrante de la Industria y para aprovechar la infraestructura y el capital humano de los centros universitarios de nivel superior y potencia la vinculación de la investigación, el desarrollo y la innovación (I+D+i) entre las universidades, los gobiernos locales, los productores de programas y aplicaciones informáticas y los centros de investigación;
8) propone las acciones que favorezcan el fortalecimiento de la empresa estatal informática y su flexibilización en la gestión económica–financiera de estas, permitiéndoles con mayor autonomía, la distribución de utilidades como salario, así como aquellas que contribuyan al incremento de los niveles de exportación de los programas y aplicaciones informáticas y servicios asociados;
9) establece, según lo regulado por el Ministerio del Comercio Exterior y la Inversión Extranjera, el procedimiento para la importación de programas o aplicaciones informáticas;
10) potencia la producción nacional para contribuir a la informatización de la sociedad y a las exigencias en materia de seguridad y soberanía tecnológica;
11) propone formas organizativas para la Industria en correspondencia con las prioridades de informatización de la sociedad y la sustitución de importaciones e implementa la migración ordenada y sostenible a plataformas de código abierto y de producción nacional;
12) prioriza la utilización de código abierto en los proyectos que desarrolle la Industria;
13) atiende el sistema de gestión integrada del capital humano específico para esta Industria que garantice su permanencia en la actividad con el fin de contribuir al mejoramiento de los procesos productivos y de servicios y minimizar el éxodo de personal.
14) atiende a los profesionales del sector informático en función del desarrollo y organización de esta Industria;
15) establece el modelo de calidad para el desarrollo de aplicaciones informáticas (MCDAI);
16) prioriza el desarrollo de las empresas vinculadas de la Industria, así como favorece la aprobación de tarifas preferenciales para los servicios asociados a las redes;
17) regula la participación de las formas de propiedad y de gestión no estatal en el desarrollo de aplicaciones y servicios informáticos;
18) promueve las asociaciones entre entidades para fortalecer la exportación de productos y servicios informáticos;
19) identifica e impulsa la ejecución de proyectos de inversión extranjera y otras formas de relación económica que potencien el mercado nacional, el crecimiento de las exportaciones y el desarrollo del capital humano;
20) fortalece las entidades especializadas de las TIC dirigidas a satisfacer las prioridades de informatización de la sociedad, la seguridad nacional, el desarrollo económico del país, la exportación de productos y servicios y potencia la vinculación de la investigación, el desarrollo y la innovación (I+D+i), así como la generación de empleos y calidad de vida;
21) impulsa la adopción de las normas técnicas internacionales y la emisión de las normas cubanas para las tecnologías, la producción y los servicios informáticos a través del fortalecimiento del

trabajo de los comités de normas técnicas;

22) establece el requisito de inscripción de los programas, aplicaciones y servicios informáticos que se desarrollen para su comercialización, en el control administrativo; así como mantiene actualizado el catálogo nacional de soluciones informáticas desarrolladas por la Industria;
23) promueve la seguridad tecnológica en los productos y los servicios informáticos;
24) prioriza el desarrollo de programas y aplicaciones informáticas de producción nacional que sean sistemas operativos, antivirus, herramientas para la planificación de recursos empresariales, plataformas de comercio y gobierno electrónico, programas y aplicaciones informáticas empotradas en equipos tecnológicos producidos en el país, que se establece como única opción de uso en el mercado nacional, excepto aquellos que se autoricen;
25) potencia el desarrollo de aplicaciones y servicios asociados al gobierno y comercio electrónico;
26) promueve la creación de plataformas que faciliten la generación y diversificación de contenidos;
27) promueve el desarrollo de la Industria de equipamiento vinculado a las TIC;
28) inserta la Industria en acuerdos generados por los mecanismos de integración regionales o internacionales para la informatización de las infraestructuras;
29) colabora en el registro y protección de la propiedad intelectual de lo que se genere en este campo para lo que tiene en cuenta las regulaciones vigentes;
30) favorece el empleo de los recursos humanos que componen la Unión de Informáticos de Cuba, como cantera para los proyectos de informatización local, nacional u otros destinados a la exportación; y
31) coordina y participa en la adecuación del marco regulatorio de la industria que contribuya a agilizar su desarrollo y organización.

Ministerios de Ciencia, Tecnología y Medio Ambiente y de Cultura:

1) Proponen o emiten las normas jurídicas relacionadas con la propiedad intelectual y el derecho de autor, respectivamente, en el ámbito del desarrollo, producción y comercialización de programas y aplicaciones informáticas, así como los mecanismos que garanticen la protección del patrimonio nacional del sector.

Ministerio de Economía y Planificación:

1) Dispone, en el marco de su competencia y según el Plan Nacional de Desarrollo Económico y Social, las medidas que favorezcan la sostenibilidad y el fortalecimiento del sistema empresarial estatal y estimulen la producción de programas, aplicaciones y servicios informáticos nacionales; y
2) establece y controla que en los estudios de factibilidad de las inversiones se tengan en cuenta los presupuestos referidos a programas y aplicaciones informáticas que permitan incrementar las capacidades en la industria nacional, reducir las importaciones, garantizar mayor seguridad nacional y generar productos exportables.

Ministerios de Educación y de Educación Superior, según corresponda:

1) Promueven la vinculación con las entidades de la Industria de los recursos humanos relacionados con la actividad de programas y aplicaciones informáticas de los centros de estudios y de investigación;
2) orientan los programas de las carreras universitarias, de los técnicos superiores y especialidades con perfiles de informática para que permitan la posterior especialización y certificación de competencia en roles profesionales y realizan su revisión periódica para lograr su actualización;
3) tramitan la homologación de cursos de formación o capacitación para que sean certificados en coordinación con entidades y universidades extranjeras;
4) promueven que los egresados de carreras universitarias afines al perfil de informática y los que laboren en las empresas del sector dominen lenguas extranjeras, preferentemente el idioma inglés;
5) garantizan la realización de cursos de formación de postgrado en las TIC para los graduados de otras disciplinas con vistas a elevar el número de expertos;
6) establecen cursos de capacitación para mejorar el desempeño y capacidad del personal de la administración estatal y local en la utilización de productos informáticos de producción nacional para la gestión estatal;
7) desarrollan acciones que impulsen la investigación-desarrollo producción de programas, aplicaciones y servicios informáticos y contribuye a la introducción de estos resultados;
8) fomentan programas de calificación y adiestramiento, con el objeto de ampliar y actualizar la especialización en las diferentes ramas de la Industria, y enfatizan lo relacionado con la ciberseguridad; a su vez promueven el desarrollo profesional y técnico y los programas de apoyo a la educación tecnológica en la esfera de la informática, en coordinación con las instituciones de educación media y superior del país;
9) implementan programas de capacitación en las diferentes ramas de esta industria, acorde con su desarrollo y evolución tecnológica;
10) mantienen relaciones con las entidades de la Industria que gestionan, producen, desarrollan programas y aplicaciones informáticas y servicios al sector educacional; y
11) desarrollan la preparación permanente del personal asociado a las TIC y a la población en general.

Ministerio de Finanzas y Precios:

1) Implementa mecanismos fiscales que estimulen el desarrollo y la comercialización de la Industria para el mercado nacional y la exportación.

Banco Central de Cuba:

1) Realiza las acciones que se requieran a fin de destinar créditos para el desarrollo de la Industria de programas y aplicaciones informáticas, de acuerdo con lo establecido en materia crediticia.

CAPÍTULO IV
DE LAS OBLIGACIONES, CAPACITACIÓN, INVESTIGACIÓN, DESARROLLO E INNOVACIÓN TECNOLÓGICA

Sección Primera
De las obligaciones de las entidades y del sistema empresarial vinculadas con la Industria

Artículo 12. Las entidades de la Industria fortalecen sus estructuras y servicios basadas en el uso integrado de las TIC.

Artículo 13. Los dispositivos Informáticos son aquellos aparatos tecnológicos que permiten el procesamiento y almacenamiento de la información y la comunicación.

Artículo 14. La Industria y las empresas dedicadas a la producción, importación y comercialización de dispositivos informáticos suscriben acuerdos en interés de favorecer la incorporación de los programas y aplicaciones informáticas desarrolladas en el país.

Artículo 15. Las empresas dedicadas a la producción de dispositivos informáticos en el país garantizan que estos equipos incorporen programas y aplicaciones informáticas de producción nacional.

Artículo 16. Se exceptúan de cumplir lo regulado en el artículo anterior aquellos dispositivos informáticos destinados a la exportación u otros que se autoricen por el Ministro de Comunicaciones.

Artículo 17. Las empresas de la Industria crean capacidades para la prestación de servicios profesionales en materia de consultoría, auditoría, capacitación y entrenamiento.

Artículo 18. Las entidades y el sistema empresarial relacionados con la Industria, implementan las acciones que se corresponden con el programa vigente de investigación, desarrollo e innovación.

Sección Segunda
De las obligaciones de los ministerios de Ciencia, Tecnología y Medio Ambiente, Comunicaciones, Educación y de Educación Superior

Artículo 19. El Ministerio de Ciencia, Tecnología y Medio Ambiente, en coordinación con los organismos de la Administración Central del Estado y el Banco Central de Cuba, establece el programa de ciencia, tecnología e innovación de la Industria, que aproveche las potencialidades del capital humano, en especial las universidades y centros de investigación.

Artículo 20. Los ministerios de Educación y de Educación Superior:

a) Validan los programas de las carreras en la especialidad de informática, que permitan la especialización y certificación de competencias en roles profesionales, en los niveles medio

superior y superior, así como la homologación de los cursos de formación o certificación a cualquier nivel, con entidades y universidades certificadas internacionalmente;

b) combinan la formación, la producción, investigación e innovación y las vinculan con las entidades de la Industria para elevar la calidad de las soluciones informáticas nacionales; y

c) potencian, en coordinación con el Ministerio de Comunicaciones, la capacitación en centros de formación, para lo que tienen en cuenta las normas internacionales, con el objetivo de atraer a personal extranjero a estos centros de formación.

Artículo 21. El Ministerio de Comunicaciones, en coordinación con los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, contribuye a la capacitación del personal en la utilización de programas y aplicaciones informáticas de producción nacional para la gestión de gobierno.

CAPÍTULO V INDUSTRIA CUBANA DE PROGRAMAS Y APLICACIONES INFORMÁTICAS PARA LA DEFENSA Y SEGURIDAD NACIONAL

Artículo 22. Los ministerios de Comunicaciones, del Interior y de las Fuerzas Armadas Revolucionarias, coordinan y establecen las acciones que permiten alcanzar paulatinamente las condiciones de fiabilidad, estabilidad y seguridad de los programas, aplicaciones y servicios informáticos que respalden la Seguridad y Defensa Nacional.

Artículo 23. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, organizan y establecen los servicios que brinde su Industria, para responder a las necesidades que el país requiera en las diferentes situaciones excepcionales y las vinculadas a la Seguridad y Defensa Nacional.

CAPÍTULO VI
REGULACIÓN, CONTROL Y FISCALIZACIÓN

Artículo 24. El Ministerio de Comunicaciones dispone de las unidades organizativas y entidades que garanticen la regulación, control y fiscalización con el fin de asegurar el cumplimiento de lo que establece el presente Decreto.

Artículo 25. Corresponde a los organismos de la Administración Central del Estado y al Banco Central de Cuba establecer el marco legal que sustente el proceso de ordenamiento en las entidades subordinadas, adscritas, atendidas y patrocinadas relacionadas con la Industria e implementar el control y la fiscalización que corresponda.

Artículo 26. Las personas naturales y jurídicas sometidas a inspección en la esfera de la Industria colaboran y facilitan la gestión de los funcionarios de las correspondientes entidades y unidades organizativas de control y fiscalización sin perjuicio de los derechos legalmente reconocidos.

Artículo 27. Las autoridades de orden público prestan la protección y auxilio a los funcionarios de las entidades y unidades organizativas de control y fiscalización que realizan la inspección en la esfera de la Industria.

DISPOSICIÓN ESPECIAL

ÚNICA: Los ministros de las Fuerzas Armadas Revolucionarias y del Interior quedan facultados para adecuar en sus sistemas lo establecido en el presente Decreto.

DISPOSICIÓN TRANSITORIA

ÚNICA: Los órganos, organismos de la Administración Central del Estado y el Banco Central de Cuba ejecutan las medidas necesarias para la migración a la utilización de programas y aplicaciones informáticas de producción nacional antes de que hayan transcurrido tres (3) años, contados a partir de la fecha de entrada en vigor del presente Decreto; y cuando no puedan cumplir con el término establecido, solicitan prórroga al Ministro de Comunicaciones, el que queda facultado para establecer el nuevo término.

DISPOSICIONES FINALES

PRIMERA: Los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular que correspondan, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización y establecen las coordinaciones que resulten necesarias relativas a la aplicación del presente Decreto.

SEGUNDA: El glosario de términos y definiciones anexo forma parte del contenido del presente Decreto.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, a los 31 días de mes de mayo de 2019.

Miguel Díaz-Canel Bermúdez
Presidente del Consejo de Ministros

JORGE LUIS PERDOMO DI-LELLA
Ministro de Comunicaciones

ANEXO
GLOSARIO DE TÉRMINOS Y DEFINICIONES

1) Entidad: Todos los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro y las organizaciones políticas, sociales y de masas.

2) Órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular: Todos los órganos superiores del Estado y del Gobierno, los órganos locales del Poder Popular, los organismos de la Administración Central del Estado y las organizaciones superiores de dirección empresarial, que incluye a la Empresa de Telecomunicaciones de Cuba S.A.

ACUERDO No. 8611/2019

El Secretario del Consejo de Ministros

CERTIFICA

POR CUANTO: El desarrollo de la infraestructura de conectividad de banda ancha nacional respalda la política a seguir con el fin de lograr mayores capacidades de transmisión de datos y potencialidades para la gestión y control de las redes de telecomunicaciones, que sirva de soporte para la Informatización de la sociedad.

POR CUANTO: Resulta necesario organizar, regular y trazar las líneas para el desarrollo integral de la banda ancha nacional, mediante la aprobación de la Estrategia de Desarrollo de la Banda Ancha en Cuba, que sirva de guía a las entidades nacionales y a la población en el desarrollo, explotación y utilización de los servicios de comunicaciones, así como encargar al Ministro de Comunicaciones con el control de su implementación y de la emisión de las disposiciones normativas complementarias que se requieran para su ejecución ordenada.

POR TANTO: El Consejo de Ministros, en el ejercicio de las facultades otorgadas por el Artículo 137, incisos ñ) y o) de la Constitución de la República de Cuba y de conformidad el Decreto-Ley No. 272 “De la Organización y Funcionamiento del Consejo de Ministros”, del 16 de julio de 2010, adoptó el 31 de mayo de 2019 el siguiente:

ACUERDO

PRIMERO: Aprobar la Estrategia de Desarrollo de la Infraestructura de Banda Ancha en Cuba en correspondencia con el Plan Nacional de Desarrollo Económico y Social hasta 2030, que se anexa al presente y que forma parte integrante de este.

SEGUNDO: Encargar al Ministro de Comunicaciones el control de la implementación de lo dispuesto en el apartado Primero y de la emisión de las disposiciones normativas complementarias que se requieran para su ejecución ordenada.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Y para remitir copia a los miembros del Consejo de Ministros, se expide la presente certificación en el Palacio de la Revolución, a los 31 días del mes de mayo de 2019. “AÑO 61 DE LA REVOLUCIÓN”.

José Amado Ricardo Guerra

ANEXO ACUERDO No. 8611

ESTRATEGIA DE DESARROLLO DE LA INFRAESTRUCTURA DE BANDA ANCHA EN CUBA

1. Objetivo

Maximizar el impacto de las telecomunicaciones y las tecnologías de la información y la comunicación, en lo adelante TIC, en la transformación y modernización de la economía y la sociedad cubana así como en la Seguridad y Defensa Nacional, mediante el empleo eficaz e intensivo de las nuevas tecnologías por los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba y demás instituciones nacionales, los órganos locales del Poder Popular, el sistema empresarial, las unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las formas de propiedad y gestión no estatal, las empresas mixtas, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas, la población en correspondencia con la disponibilidad financiera del país.

2. Alcance

La implementación de la presente estrategia se establece en el marco de una proyección hacia el 2030.

3. Definición de Banda Ancha para Cuba

A los efectos del presente documento, se define como “Banda Ancha” a la tecnología de transmisión de datos que nos permite descargar contenidos, datos, voz y video, de forma simultánea.

4. Modelo de implementación

La prestación de servicios de Banda Ancha, requiere de una estructura de red dotada de elementos tecnológicos con mayores capacidades de transmisión y potencialidades para su gestión y control.

La elaboración de un Modelo Tecnológico tiene como objetivo definir la infraestructura que se requiere para la prestación de los servicios propuestos.

Como elemento estratégico debe lograrse una sinergia en el aprovechamiento óptimo de los recursos económicos invertidos por el país en los diferentes sectores, que empleados convenientemente y con alianzas adecuadas para su explotación y comercialización, pueden ser estructuras que soporten los servicios de banda ancha, evitándose así inversiones duplicadas.

4.1 Los principales elementos del Modelo Tecnológico son:

a) Fortalecer la red de acceso con el empleo de las tecnologías disponibles en correspondencia con las particularidades de cada territorio o localidad;
b) desarrollar la capa de agregación en interés de incrementar las capacidades de la red de acceso, en especial las radiobases de la telefonía móvil; y
c) mejorar y ampliar la capacidad de la red de transporte del dorsal nacional de fibra óptica en correspondencia con la demanda de ancho de banda que se requiera.

Los órganos, organismos de la Administración Central del Estado, las entidades, los órganos locales del Poder Popular y el Banco Central de Cuba aseguran las acciones necesarias, con el objetivo de alcanzar, de manera acelerada, el uso progresivo de la Banda Ancha y el incremento del acceso de la población a los servicios asociados a la informatización de la sociedad.

4.1.1 Acciones Generales

a) Adecuar el marco regulatorio vigente a los nuevos escenarios y a la introducción de nuevas tecnologías;
b) desarrollar el aprovechamiento óptimo de las fibras ópticas desplegadas y las previstas a desplegar, así como de otros recursos y facilidades asociadas a las telecomunicaciones y las TIC;
c) fortalecer la capacidad ejecutora del país para facilitar la implementación de la infraestructura de telecomunicaciones en general y en particular de la red para la Banda Ancha;
d) organización y migración gradual de la red al protocolo IPv6, tanto en el acceso como en la capa de transporte;
e) elevar las acciones de formación y capacitación de especialistas en el sector de las Telecomunicaciones y las TIC;
f) introducir gradualmente en el mercado cubano terminales con precios asequibles que soporten los servicios de Banda Ancha;
g) desarrollar la Red Nacional de Educación e Investigación y su conexión con las redes internacionales de educación e investigación.

4.1.2 Acciones específicas. Redes fijas

a) Priorizar el despliegue de las redes provinciales y municipales, que tiene en cuenta, en primer orden, garantizar los anchos de banda requeridos para la conectividad de las radiobases de tecnología 3G y 4G así como los controladores de acceso de las redes WiFi;
b) comenzar el despliegue de las tecnologías alámbricas en aquellas áreas con redes de cobre

flexible;

c) iniciar el despliegue de redes de fibra óptica hasta el lugar (comunidad, edificio, hogar) con empleo de la tecnología de fibra óptica pasiva (GPON), y priorizar aquellas áreas con mayor densidad de población donde no existan otros servicios y aquellas en las que el impacto socioeconómico sea elevado;
d) incorporar en la red nuevas tecnologías flexibles y compactas, que faciliten su rápido despliegue y menores costos, que eviten además las construcciones civiles de alta complejidad;
e) comenzar la migración paulatina de los actuales servicios conmutados de baja velocidad hacia servicios de banda ancha;
f) continuar el despliegue de gabinetes inteligentes y redes de cobre flexibles, y mantener como política que los gabinetes que se adquieran garanticen servicios de telefonía fija y de datos así como priorizar este en las áreas con mayor densidad de población donde no exista ningún tipo de servicio;
g) comenzar el despliegue de la tecnología por cables de cobre (xDSL) en aquellas áreas donde existan las condiciones técnicas;
h) comenzar el despliegue de redes de fibra óptica hasta el usuario (FTTx) principalmente en aquellas áreas en las que el impacto socioeconómico sea elevado;
i) incorporar en los requerimientos constructivos del Instituto de Planificación Física para el diseño de edificaciones y comunidades los elementos técnicos para el despliegue de redes de fibra óptica y otras facilidades de telecomunicaciones;
j) realizar el despliegue de soluciones combinadas de tecnologías de fibra óptica y cobre.

4.1.3 Acciones específicas. Redes inalámbricas

a) Realizar el despliegue de radiobases de banda ancha móvil en la capital del país y capitales provinciales, que prioricen aquellas en las que exista conectividad por fibra óptica;
b) impulsar el despliegue de redes WiFi con prioridad en la capital del país, en las capitales provinciales, en las zonas turísticas y en las áreas de alta densidad de usuarios;
c) evaluar el empleo de otras tecnologías que brinden conectividad en las comunidades, con prioridad para estos enlaces dirigido al sector de la educación y la salud;
d) desplegar la tecnología 4G en zonas de alta demanda de tráfico de datos;
e) incrementar el servicio de acceso a Internet sobre tecnología 3G para usuarios nacionales;
f) coubicar radiobases de tecnología móvil en los sitios de la red troncalizada ferroviaria, con el objetivo de aprovechar la infraestructura existente en estos sitios y garantizar este servicio a las localidades aledañas a la red ferroviaria;
g) adquirir tecnologías que aseguren su migración hacia los estándares de 4G y superior;
h) instalar radiobases de nueva generación en las zonas de alto tráfico de voz y datos y reinstalar las que se sustituyan, para garantizar voz y datos en aquellos lugares de insuficiente cobertura;
i) preparar la migración de la red de interconexión de las radiobases a la tecnología IP, y dejar la tecnología actual como redundancia de estas con el Nodo Central del Sistema;
j) implementar soluciones con celdas pequeñas, para mejorar la cobertura de la red móvil, tanto en interiores como en áreas exteriores donde no haya cobertura o exista congestión de las macro celdas, lo que permite aliviar el tráfico de la red celular.

4.1.4 Acciones específicas. Empleo del espectro radioeléctrico

a) Emplear la banda de 1800 MHz (3 canales de 20 MHz) para el despliegue de las tecnologías de 3G y 4G, fundamentalmente para zonas urbanas de alta densidad poblacional;
b) reservar segmento en la banda de 1800 MHz para el despliegue de las tecnologías de 3G y 4G en interés de usuarios itinerantes que emplean las bandas de Servicios Inalámbricos Avanzados;
c) reservar (en el proceso del "apagón de la TV analógica") la banda de 700 MHz para el despliegue de tecnologías de 3G y 4G, con el objetivo de asegurar la conectividad en las zonas urbanas de baja densidad poblacional y comunidades;
d) evaluar la reutilización de los segmentos de banda asignados a la difusión de la TV, con el objetivo de brindar conectividad en las comunidades.

4.1.5 Acciones específicas. Desarrollo de las redes de agregación, borde y el dorsal nacional

a) Actualizar y ampliar las capacidades de la Red Dorsal Principal en correspondencia con la demanda;
b) efectuar el despliegue de redes territoriales (provinciales y municipales) en base a redes ópticas de mayor ancho de banda y flexibilidad de conexión;
c) mantener actualizados los protocolos técnicos que permiten el encaminamiento de la transmisión en paquete;
d) fortalecer gradualmente, según la demanda, la Red de Transmisión Internacional avanzando en la migración total a la tecnología IP;
e) asegurar en la arquitectura de la red de telecomunicaciones, los niveles de redundancia requeridos en la Dorsal Principal y en los restantes elementos de red que lo justifiquen (centros de datos, plataformas de control, etc.) para la disminución de vulnerabilidades;
f) incrementar la seguridad de las soluciones de fibras ópticas pasivas mediante configuraciones de anillo.

4.1.6 Acciones específicas. Desarrollo de la capa de gestión, control y supervisión

a) Considerar, en el proceso de migración del control de la red hacia el subsistema de servicios multimedia, los elementos tecnológicos necesarios para el incremento de los servicios de Banda Ancha;
b) adquirir los medios necesarios (equipos y programas de aplicación) para la medición y control de la calidad de los servicios que se prestan;
c) mantener actualizados los planes de señalización, asignación de direcciones IP, sincronización, asignación de bandas de frecuencias y transmisión;
d) actualizar periódicamente el sistema de gestión de todas las capas de red que componen la infraestructura de Banda Ancha.

5. Metas y objetivos específicos para el desarrollo de la Banda Ancha en Cuba

Las metas y objetivos específicos a alcanzar por etapas, en el desarrollo de la Banda Ancha se aprueben por el Consejo de Ministros a propuesta del Ministerio de Comunicaciones, que tiene en cuenta las posibilidades económicas del país.

El Ministerio de Comunicaciones establece los indicadores que permitan evaluar el nivel de cumplimiento de las metas y objetivos, así como las velocidades de conexión mínimas a considerar como banda ancha, de acuerdo con la evolución tecnológica que el país alcance de forma paulatina.

2. SOPORTE, RECURSOS E INFRAESTRUCTURA DE ACCESO

RESOLUCIÓN No. 22/2022

POR CUANTO: El Decreto-Ley 35 De las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y el uso del espectro radioeléctrico, de 13 de abril de 2021, dispone en su Artículo 61, que el Ministerio de Comunicaciones establece la estrategia, regulación, control del uso y administración de los recursos de Internet, que se conocen como direcciones IP, número de sistema autónomo, nombres de dominio y la resolución inversa de direcciones IP.

POR CUANTO: La Resolución 157 de 14 de agosto del 2008, del Ministro de la Informática y las Comunicaciones, establece el procedimiento para la propuesta y aprobación de nuevos dominios de categorías genéricas de segundo nivel bajo el .cu no operados por el Centro Cubano de Información de Red; la Resolución 13 de 16 de enero de 2012, del Ministro de la Informática y las Comunicaciones, aprueba como dominios genéricos de segundo nivel bajo el .cu, el dominio cult.cu y el dominio sld.cu; la Resolución 43 de 19 de febrero de 2013, del Ministro de la Informática y las Comunicaciones, aprueba como dominios genéricos de segundo nivel bajo el .cu, el dominio tur.cu y el dominio co.cu.

POR CUANTO: Se hace necesario actualizar y unificar el contenido de regulación de las mencionadas normas; así como el Procedimiento para la propuesta y aprobación de nuevos dominios de categorías genéricas de segundo nivel, los deberes y las condiciones tecnológicas con las que deben operar estos dominios en el territorio nacional, de no ponerse operativos en el Centro Cubano de Información de Red.

POR TANTO: En el ejercicio de las atribuciones que están conferidas, en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Establecer el Procedimiento para la propuesta y aprobación de nuevos dominios genéricos de segundo nivel bajo el dominio punto cu, en lo adelante .cu, así como los deberes y las condiciones tecnológicas con las que deben de operar estos dominios en el territorio nacional, de no ponerse operativos en el Centro Cubano de Información de Red, en lo adelante, CUBANIC.

SEGUNDO: Son dominios genéricos que operan bajo el .cu, los nombres genéricos de hasta 4 caracteres latinos bajo el cual se agrupa un concepto de ordenamiento de dominio, para un sistema o sector de la sociedad.

TERCERO: Los dominios genéricos de segundo nivel se aprueban mediante Resolución ministerial.

CUARTO: La persona jurídica interesada en solicitar ante el CUBANIC, un dominio genérico de segundo nivel, debe entregar la documentación siguiente:

1) Planilla de fundamentación del nuevo dominio de categoría genérica, que se adjunta en el Anexo Único de la presente Resolución.

2) Carta – aval del jefe del órgano u organismo de la Administración Central del Estado al que pertenece la entidad que propone el nuevo dominio; si este abarca a más de un sector u organismo, deben presentarse cartas – avales de éstos, que expresen su conformidad.

QUINTO: El CUBANIC cumple con los trámites establecidos para evaluar la solicitud presentada y remite sus consideraciones a la Dirección de Regulaciones del Ministerio de Comunicaciones con vista a su análisis y presentación de la propuesta al que suscribe, para su aceptación o no en un plazo de 30 días; las conclusiones de este proceso se comunican al solicitante, a la Dirección General de Informática y al CUBANIC.

SEXTO: La persona jurídica cubana que recibe autorización para registrar a su nombre el nuevo dominio genérico de segundo nivel, tiene los deberes siguientes:

a) Cumplir con lo establecido para la operación de nombres de dominios;

b) realizar los registros de dominio a él autorizado y publicarlos en una página web;

c) elaborar las normas por las cuales se inscriben nuevos dominios y tener en cuenta los nombres de dominio internacionalizados, así como las regulaciones establecidas en el CUBANIC;

d) establecer y divulgar los procedimientos de solución de disputa sobre dominios y de mediación y arbitraje;

e) establecer la promoción y mantenimiento del registro a su cargo, donde se hagan constar los horarios de actualizaciones de zonas y activaciones de dominio.

SÉPTIMO: La persona jurídica que opere un dominio genérico de segundo nivel y que no esté operado por el CUBANIC, tiene que cumplir con las condiciones tecnológicas que se relacionan a continuación:

a) Establecer y operar la infraestructura tecnológica necesaria que garantice el buen funcionamiento de la operación del registro y la operación de los servidores de dominios, primarios y secundarios;

b) coordinar con el CUBANIC el funcionamiento del dominio genérico asignado;

c) realizar los cambios tecnológicos necesarios que garanticen un funcionamiento actualizado y adecuado del servicio que presta;

d) establecer, en correspondencia con las disposiciones jurídicas vigentes, las medidas de seguridad y planes de contingencias relacionados con el servicio que presta;

e) garantizar la operación y el servicio del dominio genérico asignado las 24 horas del día y todos los días del año.

OCTAVO: El CUBANIC debe verificar que los dominios genéricos de segundo nivel aprobados que operan fuera de este, cumplen con lo establecido en la legislación vigente.

NOVENO: Mantener como dominios genéricos de segundo nivel bajo el .cu no operados por el CUBANIC los siguientes:

a) cult.cu, que agrupa a las entidades relacionadas con el sector de la cultura y es operado por el Centro de la Informática y Sistemas Aplicados a la Cultura, CUBARTE;

b) sld.cu, que agrupa a las entidades relacionadas con el sector de la salud y es operado por el Centro Nacional de Información de Ciencias Médicas, INFOMED;

c) tur.cu, que agrupa a las entidades relacionadas con el sector del turismo y es operado por la Empresa de Servicios Informáticos para el Turismo, GET;

d) co.cu, que agrupa a las redes corporativas de las entidades que reciben como parte de los servicios, la asignación de nombres de dominio de la Empresa de Telecomunicaciones de Cuba, S.A., como proveedor de servicios públicos y es operado por esta.

DÉCIMO: Le corresponde al Centro de la Informática y Sistemas Aplicados a la Cultura, al Centro Nacional de Información de Ciencias Médicas y a la Empresa de Servicios Informáticos para el Turismo, mantener de forma automatizada el registro del dominio autorizado hasta el cuarto nivel; y a la Empresa de Telecomunicaciones de Cuba, S.A hasta el tercer nivel y todos deben brindar la información que se solicite por las autoridades facultadas.

UNDÉCIMO: El incumplimiento de lo dispuesto en la presente Resolución, se informa al jefe de la entidad que participa en este proceso, con copia al jefe del órgano u organismo de la Administración Central del Estado correspondiente.

DISPOSICIONES FINALES

PRIMERA: La Dirección General de Informática y la Dirección de Inspección, del Ministerio de Comunicaciones, son las encargadas del control y la supervisión de lo dispuesto en la presente Resolución.

SEGUNDA: Derogar las Resoluciones, 157 de 14 de agosto del 2008, la 13 de 16 de enero de 2012 y la 43 de 19 de febrero de 2013, todas del Ministro de la Informática y las Comunicaciones.

DÉSE CUENTA a los ministros de Cultura, de Salud Pública, de Turismo y de Ciencia, Tecnología y Medio Ambiente.

NOTIFÍQUESE al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A.; a los presidentes de los Grupos Empresariales de Ciencia Tecnología y Medio Ambiente, INNOMAX y de Servicios al Turismo, SERVITUR; y a los directores del Centro de la Informática y Sistemas Aplicados a la Cultura, del Ministerio de Cultura, y del Centro Nacional de Información de Ciencias Médicas, del Ministerio de Salud Pública.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones y de la Oficina para la Seguridad de las Redes Informáticas y al Director de Regulaciones, todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 9 del mes de marzo del 2022

Mayra Arevich Marín

ANEXO ÚNICO

PLANILLA DE FUNDAMENTACIÓN DEL NUEVO DOMINIO DE CATEGORÍA GENÉRICA

Nombre de la Entidad:	
Dirección:	
Teléfono:	
Contacto Administrativo:	
Teléfono y correo electrónico:	
Contacto Técnico:	
Teléfono y correo electrónico:	
Nombre de dominio solicitado:	
Fundamento de la solicitud:	

RESOLUCIÓN No. 20/2022

POR CUANTO: El Decreto-Ley 35 De las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y el uso del espectro radioeléctrico, de 13 de abril de 2021, en su artículo 61 dispone que el Ministerio de Comunicaciones establece la estrategia, regulación, control del uso y administración de los recursos de Internet, que se conocen como direcciones IP, número de sistema autónomo, nombres de dominio y la resolución inversa de direcciones IP.

POR CUANTO: La Resolución 150 de 24 de julio de 2008, del Ministro de la Informática y las Comunicaciones, dispone que el CUBANIC de la República de Cuba, es el responsable por la correcta administración y gestión del dominio punto cu; la Resolución 103 de 16 de junio de 2011, del Ministro de la Informática y las Comunicaciones, establece que se incorpore al Sistema de Nombres de Dominio de la República de Cuba el Registro de Nombres de Dominios Internacionalizados de Segundo Nivel bajo el punto cu con caracteres multilingües propios del idioma español; la Resolución 220 de 11 de diciembre de 2012, del Ministro de la Informática y las Comunicaciones, aprueba el cambio del dominio genérico de segundo nivel ".gov.cu" por el de ".gob.cu"; la Resolución 280 de 30 de octubre de 2015, del Ministro de Comunicaciones, aprueba el Dominio Genérico de segundo nivel nat.cu definido para personas naturales residentes en el país.

POR CUANTO: Debido al desarrollo y organización alcanzado en esta materia, resulta necesario actualizar y unificar las mencionadas normas jurídicas.

POR TANTO: En el ejercicio de las atribuciones conferidas, en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Mantener al Centro de Información de Red de la República de Cuba, en lo adelante CUBANIC, como el responsable de la administración y gestión del dominio punto cu, en lo adelante .cu; del funcionamiento de los servidores de nombre de dominios primarios y secundarios; del Registro de nombres de dominios de segundo nivel bajo el .cu, así como, del Registro de los dominios de categorías genéricas bajo el .cu a él asignados.

SEGUNDO: Al nombre que se utiliza para identificar recursos en una red, una terminal o varias terminales en red o un sitio en Internet, que facilitan la memorización de las direcciones, se denomina nombre de dominio; los cuales constan de nombres separados por punto.

TERCERO: Se entiende por dominio geográfico, de código de país o de nivel superior de código de país, también conocido como Country Code Top Level Domain, por sus siglas en inglés, ccTLD, al dominio de dos caracteres de longitud, usado y reservado para un país, región o territorio dependiente, que corresponden a la norma ISO-3166-1.

CUARTO: Los servidores primarios o principales de nombres de dominios, son los que almacenan la base de datos distribuida, donde los nombres de dominio son asociados a determinados recursos de Internet; los servidores secundarios de nombres de dominio actúan como servidores de reserva para el servidor primario de la misma zona, si no se puede tener acceso al servidor principal o éste se encuentre inactivo.

QUINTO: Se considera nombre de dominio de segundo nivel, aquel que se escribe inmediatamente antes del dominio de primer nivel.

SEXTO: Son dominios genéricos que operan bajo el .cu, los nombres genéricos de hasta 4 caracteres latinos bajo el cual se agrupa un concepto de ordenamiento de dominio, para un sistema o sector de la sociedad.

SÉPTIMO: Mantener como dominios genéricos de segundo nivel bajo el .cu y administrados por el CUBANIC, los siguientes:

a) edu.cu: para definir centros del sistema de Educación;

b) com.cu: para personas jurídicas con actividades comerciales de bienes y servicios con fines de lucro;

c) net.cu: para Proveedores Públicos de Telecomunicaciones;

d) org.cu: para Organizaciones no gubernamentales y sin fines de lucro;

e) gob.cu: para órganos y organismos de la Administración Central del Estado y otras estructuras de Gobierno;

f) inf.cu: para entidades relacionadas con la actividad de información científica y proveedores de información o contenidos;

g) nat.cu: para personas naturales residentes en el país.

OCTAVO: Las personas naturales residentes en el país también pueden solicitar la titularidad de nombres de dominio bajo el .cu.

NOVENO: Las Normas del CUBANIC para su funcionamiento, se establecen en el Anexo Único de la presente Resolución.

DÉCIMO: El CUBANIC tiene la obligación de verificar los nuevos dominios de categorías genéricas que se creen fuera de este, que funcionen técnicamente de manera óptima, para lo cual emite el dictamen correspondiente antes del inicio de la entrada en explotación del dominio.

DISPOSICIONES FINALES

PRIMERA: La Dirección General de Informática y la Dirección de Inspección, del Ministerio de Comunicaciones, son las encargadas del control y supervisión de lo dispuesto en la presente Resolución.

SEGUNDA: Derogar las Resoluciones, 150 de 24 de julio de 2008, 103 de 16 de junio de 2011 y 220 de 11 de diciembre de 2012, todas del Ministro de la Informática y las Comunicaciones, y la 280 de 30 de octubre de 2015, del Ministro de Comunicaciones.

DÉSE CUENTA a la ministra de Ciencia, Tecnología y Medio Ambiente.

NOTIFÍQUESE al Presidente del Grupo Empresarial de Ciencia Tecnología y Medio Ambiente, INNOMAX; al Director General de Informática y al Director de Inspección, del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones y de la Oficina de Seguridad para las Redes Informáticas y al Director de Regulaciones, todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 9 del mes de marzo del 2022

Mayra Arevich Marín

ANEXO ÚNICO

NORMAS DEL CUBANIC

DISPOSICIONES GENERALES

1. El Registrador

1.1. La Empresa de Tecnologías de la Información y Servicios Telemáticos Avanzados, conocida por CITMATEL, tiene a su cargo el CUBANIC y los servidores primarios y secundarios del .cu de Internet, según las disposiciones jurídicas vigentes.

1.2. El CUBANIC es el responsable de otorgar e inscribir en el Sistema de Nombres de Dominio.cu, los nombres de dominio de segundo nivel bajo el indicativo del país, cu; y de tercer nivel bajo los dominios genéricos de segundo nivel por él administrados: edu, gob, org, inf, net, com y nat, según se indica en la clasificación de dominios bajo .cu.

1.3. Estas Normas establecen el conjunto de reglas o preceptos a seguir para la solicitud, otorgamiento, renovación, modificación, transferencia, suspensión y cancelación vigentes para nombres de dominio bajo el indicativo de país cu.

DE LOS NOMBRES DE DOMINIO

2. Solicitud

2.1. El CUBANIC otorga la titularidad de un nombre de dominio a la primera persona natural o jurídica en pleno ejercicio de su capacidad legal que lo solicite, previo reconocimiento de que la solicitud y el solicitante cumplen con todos los requisitos establecidos en las Normas; la persona natural o jurídica a la que el CUBANIC otorgue un nombre de dominio es reconocida en lo adelante como el titular.

2.2. Pueden solicitar el otorgamiento de un nombre de dominio las personas jurídicas cubanas y extranjeras y las personas naturales residentes en el país.

2.3. En la solicitud del nombre de dominio debe tenerse en cuenta que este no es una propiedad, es sólo la inscripción en un soporte electrónico realizado a nombre de una persona, natural o jurídica, a la cual se le otorga la titularidad.

2.4. Sólo se da curso a la solicitud de otorgamiento de un nombre de dominio si éste no se encuentra previamente requerido u otorgado bajo igual categoría genérica que el solicitado.

2.5. El CUBANIC da curso a la solicitud de otorgamiento de un nombre de dominio y se reserva el derecho de negarse a realizar el trámite solicitado con el uso de su facultad de última decisión, previa consulta con las autoridades competentes.

2.6. La recepción por el CUBANIC de la solicitud de otorgamiento de un nombre de dominio no lo obliga de ninguna manera a proceder sin que antes se verifique el cumplimiento de las Normas.

2.7. El otorgamiento de un nombre de dominio tiene una vigencia de un año, renovable consecutivamente por igual período.

2.8. El titular de un nombre de dominio bajo .cu es responsable de:

a) Conocer y acatar sin reservas de ningún tipo las Normas, así como las actualizaciones y modificaciones a estas;

b) las posibles violaciones a los derechos de propiedad intelectual, u otros que puedan derivarse del uso de un nombre de dominio y sus subdominios.

2.9. Una persona puede solicitar el otorgamiento de varios nombres de dominio siempre que no tenga como objetivo prácticas monopolísticas, la especulación o competencia desleal.

2.10.1 El titular de un nombre de dominio está representado por los contactos administrativo, técnico y financiero, en una o varias personas naturales;

2.10.2 Si el dominio se otorga a persona natural los contactos coinciden con el titular y si se otorga a persona jurídica los contactos son personas naturales, que cumplen las funciones siguientes:

a) El contacto administrativo es la persona natural a la que corresponde la máxima responsabilidad por la utilización que se dé al dominio, por los datos declarados sobre el titular y los contactos; queda obligado a informar al CUBANIC cualquier variación en dichos datos.

b) el contacto técnico es la persona natural que actúa como intermediario para temas técnicos relacionados con un dominio operativo; es con quien el CUBANIC interactúa en caso de cualquier problema en la configuración u operación del dominio en cuestión.

c) el contacto financiero es la persona natural responsable de pagar la cuota por el otorgamiento o renovación anual del dominio en la fecha que corresponda.

2.11. El CUBANIC mantiene un servicio de información web donde se publican las normas, tarifas y la relación de dominios otorgados, incluidos los datos de los titulares y sus contactos, con el consentimiento previo de estos, así como los servidores del Sistema de Nombres de Dominio, por sus siglas en inglés, DNS; esta información es publicada en www.nic.cu y www.cubanic.cu.

2.12. Todos los trámites con el CUBANIC se realizan en idioma español, salvo que sea imprescindible aceptarlo en idioma inglés.

2.13. Tanto el titular como el CUBANIC utilizan los sitios web www.nic.cu y www.cubanic.cu y el correo electrónico como medio de comunicación oficial para los trámites de solicitud,

actualización, modificación o envío de avisos de pago y además para reclamaciones o información de disputas; el CUBANIC acepta el envío de documentos en formato digital, siempre que estos tengan como origen los declarados por el titular o el contacto administrativo del dominio; en casos donde el intercambio de documentos físicos sea necesario, se emplea el correo certificado o la entrega personal.

3. Requisitos para el otorgamiento

3.1. Los nombres de dominio tienen establecidas como reglas de sintaxis las siguientes:

a) Los caracteres válidos para un nombre de dominio son las letras del alfabeto castellano, de la a hasta la z, los dígitos arábigos, del 0 al 9, el guión "-" y los caracteres á, é, í, ó, ú, ü y ñ; los cuales al ser incluidos en los nombres de dominio se denominan nombres de dominio internacionalizados. No se hace distinción entre mayúsculas y minúsculas;

b) los nombres de dominio no deben comenzar o terminar con el guión "-" ni presentar dos guiones seguidos "--" en su constitución;

c) la longitud mínima para un nombre de dominio de segundo nivel bajo .cu, o de tercer nivel bajo subdominios de categorías genéricas bajo .cu, es de tres caracteres, aunque se recomiendan cinco caracteres como mínimo;

d) la longitud máxima admitida para un nombre de dominio de segundo nivel bajo .cu o de tercer nivel bajo subdominios de categorías genéricas bajo .cu, es de 63 caracteres.

3.2. Los nombres de dominio tienen establecidas como reglas generales de derivación las siguientes:

3.2.1 Una persona jurídica puede solicitar el otorgamiento de un nombre de dominio en los casos siguientes:

a) Constituya una marca concedida al solicitante por la Oficina Cubana de la Propiedad Industrial, en lo adelante OCPI;

b) coincida plenamente con el nombre de la persona solicitante, su acrónimo, sigla o alias legalmente reconocido;

c) cualquier otro nombre que no se encuentre incluido entre los casos anteriormente citados y no constituya alguna de las excepciones previstas.

3.2.2 Una persona natural puede solicitar el otorgamiento de un nombre de dominio en los casos siguientes:

a) Constituya una marca concedida al solicitante por la OCPI;

b) cualquier otro nombre que no constituya alguna de las excepciones previstas.

3.3. Un nombre de dominio no se otorga en los casos siguientes:

a) Se componga de términos genéricos, comunes o usuales;

b) se componga de términos geográficos o gentilicios;

c) incluya, sea idéntico o engañosamente similar al nombre del país en idioma español;

d) coincida con nombres de dominio de primer nivel, genéricos de segundo nivel, protocolos, aplicaciones y terminología de Internet;

e) se componga de nombres propios, apellidos o apelativos de una persona natural, salvo que constituya una marca concedida al solicitante por la OCPI o sea una personalidad con reconocimiento por la actividad que realice;

f) incluya términos o expresiones que resulten dañinos o perjudiciales para la seguridad pública, la integridad, la ética, la moral y las buenas costumbres, la economía, la independencia y la soberanía nacional;

g) se asocie de forma pública y notoria a otra persona, acrónimo, marca u otro signo distintivo diferente de los del solicitante del nombre de dominio;

h) se componga de una secuencia de dígitos, salvo si se corresponde literalmente con una marca u otro signo distintivo registrado por el solicitante en la OCPI.

3.4. Se exceptúan de las regulaciones expresadas en el 3.3, incisos a, b, c y d, aquellas solicitudes realizadas o aprobadas por las autoridades nacionales competentes.

3.5. El solicitante está en la obligación de pagar la cuota de otorgamiento.

4. Procedimiento para el otorgamiento

4.1. La solicitud de otorgamiento de un nombre de dominio se presenta al CUBANIC por el contacto administrativo en los casos en que el solicitante sea una persona jurídica y por el propio solicitante, si se trata de una persona natural; para presentar la solicitud se utiliza el formulario de solicitud de otorgamiento, que se puede obtener en las páginas web www.nic.cu y www.cubanic.cu o solicitar por el correo nic-staff@nic.cu.

4.2. Al llenar la solicitud de otorgamiento de un nombre de dominio se declaran los datos del solicitante, de las personas naturales que actúan como contactos y de los servidores que permiten activar el dominio; el solicitante toma como nombre de usuario el nombre de dominio y define una palabra clave o contraseña que en lo adelante lo identifica plenamente para cualquier trámite relativo al dominio otorgado.

4.3. Con el fin de comprobar que un nombre de dominio no viola lo establecido en las Normas, el CUBANIC puede requerir del solicitante la presentación de los documentos siguientes, donde conste el nombre de dominio solicitado:

4.3.1 Para las personas jurídicas:

a) Registro de Marca u otro signo distintivo registrado a nombre del solicitante en la OCPI;

b) certificado de inscripción en el Registro Mercantil o Directorio de Unidades Institucionales y Establecimientos, DUINE;

c) certificado de inscripción en el Registro Nacional de Publicaciones Seriadas;

d) certificado de inscripción en el Registro Nacional de Asociaciones;

e) si el nombre de dominio solicitado no se encuentra comprendido en alguna de las anteriores opciones, el CUBANIC toma como referencia la información emitida por el Departamento de marcas y otros signos distintivos de la OCPI donde se verifique la no coincidencia del nombre de dominio solicitado con nombres registrados en el país por otra persona jurídica o natural diferente del solicitante.

4.3.2 Para las personas naturales:

a) Registro de Marca u otro signo distintivo registrado por el solicitante en la OCPI;

b) documento que avale el reconocimiento en la actividad que es considerado personalidad.

c) si el nombre de dominio solicitado no se encuentra comprendido en alguna de las anteriores opciones, el CUBANIC toma como referencia la información emitida por el Departamento de marcas y otros signos distintivos de la OCPI donde se verifique la no coincidencia del nombre de dominio solicitado con nombres registrados en el país por otra persona jurídica o natural diferente del solicitante.

4.4. Para determinar si un nombre de dominio está solicitado u otorgado, se considera que un nombre de dominio internacionalizado es semejante a dicho nombre escrito con caracteres tradicionales; o sea que las letras acentuadas o con diéresis son equivalentes a dichas letras sin acento ni diéresis; de igual forma se consideran las letras ñ y n.

4.5. El CUBANIC se reserva el derecho de solicitar o consultar con las autoridades competentes la información que estime pertinente con el fin de otorgar un nombre de dominio.

5. Términos para la renovación

5.1. El titular renueva un nombre de dominio anualmente; para ello como requisito indispensable está el cumplimiento de las Normas.

5.2. El CUBANIC da curso a la solicitud de renovación de un nombre de dominio de conformidad con las Normas, reservándose el derecho de negarse a realizar el trámite solicitado en uso de su facultad de última decisión, previa consulta con las autoridades competentes.

6. Derechos del titular

6.1. El otorgamiento de un nombre de dominio confiere al titular la facultad de impedir que terceros sin autorización, lo utilicen a su favor.

6.2. El titular conserva su nombre de dominio para la zona cu, independientemente de que cambie de proveedor de servicios del entorno de Internet o esté conectado a varios de ellos simultáneamente.

6.3. Una vez que se ha completado el proceso de otorgamiento de un nombre de dominio, el CUBANIC lo registra en el servidor del Sistema de Nombres de Dominio .cu y publica en su sitio web con toda la información que lo identifica, incluyendo la de sus contactos.

6.4. Es posible que un dominio no mantenga una conexión dedicada y permanente a Internet.

6.5. Para hacer efectiva la utilización de un dominio es necesario que haya sido configurado un servidor de nombres, Sistema de Nombres de Dominio primario, y opcionalmente, al menos un servidor de Sistema de Nombres de Dominio secundario.

7. De la modificación de los datos

7.1. El nombre de un dominio no puede ser modificado; para todos los efectos esto se considera como la solicitud de otorgamiento de un nuevo nombre de dominio y como tal se procede.

7.2. La modificación del nombre del titular del dominio se realiza:

a) A solicitud del titular si cambia de nombre;

b) si se transfiere la titularidad del nombre de dominio, según lo dispuesto en las Normas.

7.3. La solicitud de cambio de nombre del titular es presentada al CUBANIC por el contacto administrativo.

7.4. El CUBANIC puede solicitar los documentos que estime necesarios con el fin de comprobar que el cambio de titularidad, no viola lo establecido en la Normas.

7.5. Los datos declarados sobre un nombre de dominio relativos a la ubicación del titular, las generales de los contactos administrativo, técnico, financiero y los DNS, pueden ser modificados en todo o en parte en cualquier momento, siempre que se encuentre al corriente el pago de las tasas previstas en las normas para el registro y renovación del nombre de dominio y no medie una disputa por la titularidad.

7.6. Los contactos administrativo y técnico están facultados para solicitar las modificaciones necesarias, la que es remitida desde los correos electrónicos declarados para dichos contactos o a través de los sitios web www.nic.cu y www.cubanic.cu; en caso de no ser posible para los contactos emplear el correo electrónico, se debe presentar la solicitud por escrito mediante documento firmado por el contacto administrativo o técnico.

8. Transferencia de los nombres de dominio

8.1. La titularidad de un nombre de dominio es transferible por cualquiera de las formas admitidas en Derecho, salvo disposición en contrario.

8.2. El proceso de transferencia de titularidad de un nombre de dominio se encuentra sujeto a lo estipulado en las Normas.

8.3. El CUBANIC da curso a la solicitud de transferencia de titularidad de un nombre de dominio, reservándose el derecho de negarse a realizar el trámite solicitado en uso de su facultad de última decisión, previa consulta con las autoridades competentes.

8.4. Para la transferencia de un nombre de dominio:

a) La solicitud de transferencia de titularidad de un nombre de dominio se entrega al CUBANIC por el contacto administrativo; en el documento debe identificarse plenamente al actual titular, incluyendo su palabra clave o contraseña del dominio a transferir, y expresar plenamente su voluntad de realizar la transferencia de titularidad, así como las condiciones bajo las cuales esta se realiza, y se debe consignar las generales del nuevo titular del nombre de dominio;

b) el receptor del nombre de dominio debe cumplir con las Normas para los solicitantes de nombres de dominio;

c) el receptor del nombre de dominio debe llenar el Formulario de solicitud de otorgamiento, incluyendo una nueva palabra clave o contraseña; y

d) el receptor del nombre de dominio debe cumplir con el pago de la tarifa establecida para la renovación de este, sin detrimento de cualquier pago equivalente realizado por el anterior titular respecto al año en curso. Si así no lo hiciera dentro del plazo establecido, el CUBANIC no procede a realizar la transferencia.

8.5. El CUBANIC puede solicitar los documentos que estime necesarios con el fin de comprobar que el cambio de titularidad no viola lo establecido en las Normas.

8.6. El proceso de transferencia de un nombre de dominio a un nuevo titular queda en suspenso mientras medie un proceso de disputa por la titularidad de este o se encuentre pendiente un proceso para su revocación.

9. De la suspensión y revocación

9.1. Por suspensión de un nombre de dominio se entiende la inhabilitación de este para ser resuelto por los servidores de nombre de Internet y la incapacidad de que un tercero lo pueda solicitar.

9.2. Son causales para la suspensión de un nombre de dominio:

a) Incumplir las Normas;

b) incumplir el tiempo establecido para abonar el pago de alguna cuota;

c) proporcionar información falsa o imprecisa en la solicitud o actualización de los datos de identificación del titular o los contactos del nombre de dominio;

d) mantener desactualizada la información contenida en la base de datos del CUBANIC;

e) emitir disposición por autoridad competente;

f) incumplir con la calidad y estabilidad en el servicio de la red, cuando esto sea un requisito.

9.3. La suspensión se mantiene hasta tanto sea resuelta la causa que la motivó, siempre que no exceda los 30 días de aplicada la medida.

9.4. Por revocación de un nombre de dominio se entiende la inhabilitación del dominio para ser resuelto por los servidores de nombre de Internet y queda éste disponible para que sea solicitado por un tercero.

9.5. Son causales para la pérdida de titularidad del nombre de dominio, de oficio o a instancia de parte, cualquiera de las circunstancias siguientes:

a) La renuncia;

b) si la solicitud de otorgamiento se ha realizado de mala fe o su uso es abusivo;

c) si el otorgamiento lesiona los derechos de propiedad intelectual, supone actos de competencia desleal o vulnera derechos de terceros;

d) si con la utilización del nombre de dominio se pone en peligro el orden público, la moral, la integridad de las personas, las buenas costumbres, la seguridad nacional, o la legalidad socialista;

e) por disposición en sentencia firme o laudo arbitral;

f) por el titular haber dejado de existir;

g) por impago de la cuota de renovación anual;

h) por incompetencia o negligencia técnica reiterada en el uso del nombre de dominio o por violaciones de la seguridad tecnológica.

9.6. Las causales descritas en los incisos d, e, f, g y h del 9.5 generan la revocación de un nombre de dominio de oficio; esta revocación es informada de forma inmediata al titular mediante las vías declaradas para los contactos administrativo y técnico.

9.7. La revocación de un nombre de dominio, como resultado de una disposición judicial o de un proceso de mediación y arbitraje, se ejecuta de forma inmediata, una vez recibida por el CUBANIC la documentación correspondiente.

10. De los pagos

10.1. La recepción por el CUBANIC del pago por vía electrónica u otras establecidas, de la tarifa por el otorgamiento o renovación de un nombre de dominio, constituye la confirmación de que el titular acepta las Normas.

10.2. El CUBANIC no está obligado a activar o mantener activo, un nombre de dominio a menos que se haya realizado el pago de la cuota de otorgamiento o renovación, según sea el caso.

10.3. El titular del dominio, representado por el contacto financiero, es responsable de pagar la cuota por el otorgamiento o renovación anual en la fecha que corresponda.

10.4. Los pagos efectuados por el otorgamiento o la renovación del nombre de dominio no son reembolsables una vez que el CUBANIC haya efectuado lo solicitado.

10.5. A los efectos del pago, un Nombre de Dominio Internacionalizado se considera independiente de un nombre de dominio semejante, escrito con caracteres tradicionales.

10.6. El CUBANIC aplica dos tipos de cuotas que cubren cada una un término de 12 meses a partir del mes que consta como fecha de otorgamiento:

a) Cuota por el otorgamiento de un nuevo nombre de dominio;

b) cuota de renovación, para extender por un año el registro de un nombre de dominio otorgado.

10.7. El CUBANIC tiene la opción de enviar un aviso por vías digitales para el pago de la renovación de un dominio, al contacto financiero del titular con un plazo de hasta 30 días antes de la fecha de vencimiento del dominio.

10.8. El titular debe informar al CUBANIC su intención de pago de la renovación con no menos de 15 días antes de la fecha de vencimiento del dominio.

10.9. El impago de la renovación por el titular después de transcurridos 15 días posteriores al vencimiento del dominio, causa la suspensión del dominio.

10.10. El impago de la renovación por el titular después de transcurridos 30 días posteriores al vencimiento del dominio, causa la revocación de este.

DE LAS DISCREPANCIAS DE TITULARIDAD Y MODIFICACIÓN DE NORMAS

11. De las discrepancias por la titularidad de un nombre de dominio

11.1. Los procedimientos para el otorgamiento de nombres de dominios descritos en las Normas tienen entre sus objetivos principales evitar las causas más frecuentes de discrepancia por la titularidad de un nombre de dominio; no obstante, si las circunstancias conducen a una discrepancia, esta es ventilada en órganos de mediación y arbitraje cubanos o por la vía judicial en el territorio nacional, para lo cual se aplica la ley cubana y el idioma a utilizar es el español.

11.2. Toda persona natural o jurídica que estime afectados sus derechos por la concesión de un nombre de dominio, puede solicitar la revocación de este.

11.3. A los efectos del CUBANIC se da como fecha de comienzo de un proceso de disputa relativo a un nombre de dominio, la fecha en que el CUBANIC sea informado oficialmente de este.

11.4. Cualquier trámite de transferencia de titularidad, modificación de datos relativos a los contactos y DNS de un dominio sometido a disputa quedan bloqueados hasta que concluya dicho proceso.

11.5. A los efectos de CUBANIC, se da como fecha de conclusión de un proceso de discrepancia relativo a un nombre de dominio, la fecha en que el CUBANIC sea notificado oficialmente de este por la autoridad u organismo correspondiente.

11.6. El CUBANIC acepta el envío de documentos por vía digital o de entrega personal en formato digital; en casos donde el intercambio de documentos físicos sea necesario, se emplea el correo certificado o la entrega personal.

12. De las modificaciones a las Normas del CUBANIC

12.1. El CUBANIC puede proponer la modificación de sus Normas, las cuales son aprobadas por el Ministerio de Comunicaciones y publicadas en su sitio web www.nic.cu y www.cubanic.cu, con no menos de 30 días antes de su entrada en vigor. Adicionalmente, el CUBANIC puede enviar un aviso por correo electrónico a los titulares de nombres de dominio sobre dicha modificación.

RESOLUCIÓN No. 141/2020

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros, de 22 de mayo de 2017, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de estos.

POR CUANTO: El Decreto 359 "Sobre el Desarrollo de la Industria Cubana de Programas y Aplicaciones Informáticas" de 31 de mayo de 2019 en su Disposición Transitoria Única**,** establece que los órganos, organismos de la Administración Central del Estado y el Banco Central de Cuba ejecutan las medidas necesarias para la migración a la utilización de programas y aplicaciones informáticas de producción nacional; por lo que resulta necesario establecer las indicaciones generales para la migración hacia plataformas de código abierto y la generalización de programas y aplicaciones informáticas de producción nacional, con el objetivo de promover y priorizar su uso e incrementar la soberanía y seguridad nacional, y a su vez establecer las medidas que garanticen brindar servicios de asesoría técnica y formación del personal.

POR TANTO: En el ejercicio de las atribuciones conferidas en el Artículo 145 inciso d), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Establecer las indicaciones generales para la migración hacia plataformas de código abierto y la generalización de programas y aplicaciones informáticas de producción nacional en los sistemas operativos de los nodos tecnológicos, servidores o centros de datos privados que soportan los sistemas informáticos, así como las computadoras personales de escritorio y portátiles, que estén todos conectados a Internet, a ser aplicadas por los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, la Aduana General de la República, el Instituto de Planificación Física y la Oficina Nacional de Estadística e Información, y el cronograma general de migración que abarca el período 2021-2024, que como Anexo Único, forma parte de la presente Resolución.

SEGUNDO: Se denomina programa o aplicación informática de código abierto al que posea una licencia que permita, con mayores o menores restricciones, ejecutar, modificar y distribuir la aplicación informática y que brinda acceso a sus programas listados de códigos fuente, con reconocimiento o no del autor.

TERCERO: Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, la Aduana General de la República, el Instituto de Planificación Física y la Oficina Nacional de Estadística e Información, en relación con los programas y aplicaciones informáticas que utilizan, deben desarrollar las acciones siguientes:

a) Efectuar la migración hacia una distribución de sistema operativo en código abierto, de producción nacional, siempre que estas cumplan con los estándares de calidad y seguridad establecidos por las entidades correspondientes;
b) establecer las relaciones contractuales con los desarrolladores y entidades para garantizar la asesoría técnica, la capacitación del personal y el soporte de los programas y aplicaciones informáticas;
c) solicitar autorización a la Dirección General de Informática del Ministerio de Comunicaciones, para el uso de sistemas operativos o aplicaciones propietarias de producción nacional o extranjeras, así como de código abierto extranjero que por razones de índole técnica, económica, o jurídica justifiquen su utilización, y que cumplan con los estándares de calidad y seguridad establecidos por las entidades facultadas;
d) regirse, durante la migración hacia plataformas de código abierto, por las indicaciones metodológicas, que emita el Ministerio de Comunicaciones, las cuales deben estar disponibles en su sitio web institucional;
e) elaborar su cronograma de migración hacia plataformas de código abierto de forma tal que garantice culminar su proceso de migración en diciembre de 2024, y prever la generalización de programas y aplicaciones informáticas de producción nacional, este debe contener la forma y los plazos para ejecutar las medidas establecidas según el cronograma general que se anexa a la presente, ajustado a sus características y con identificación expresa de los responsables de cada tarea;
f) controlar y evaluar la ejecución de su cronograma de migración hacia plataformas de código abierto e informar el estado de su cumplimiento a la Dirección General de Informática, en la segunda quincena de los meses de marzo y septiembre de cada año; y
g) solicitar prórroga al que suscribe, cuando por razones justificadas no puedan cumplir el cronograma establecido, el que queda facultado para establecer el nuevo término.

CUARTO: El cronograma de migración hacia plataformas de código abierto de cada órgano, organismo de la Administración Central del Estado, el Banco Central de Cuba, la Aduana General de la República, Instituto de Planificación Física y la Oficina Nacional de Estadística e Información, se presenta al Director General de Informática, en el plazo de ciento veinte días posteriores a la fecha de la publicación de la presente Resolución en la Gaceta Oficial, y previamente aprobado por el máximo jefe de la entidad.

QUINTO: Se encarga al Director General de Informática del Ministerio de Comunicaciones, de evaluar las infraestructuras críticas de las Tecnologías de la Información y la Comunicación, de acuerdo con sus

características y condiciones, e incorporarlas al proceso de migración hacia plataformas de código abierto y a la generalización de los programas y aplicaciones informáticas de producción nacional en los sistemas operativos de los nodos tecnológicos, servidores o centros de datos privados que soportan sus sistemas informáticos y a las computadoras personales de escritorio y portátiles de estas que estén conectados a Internet.

SEXTO: Las infraestructuras críticas de las Tecnologías de la Información y la Comunicación, que como resultado de la referida evaluación, se consideren incorporar al proceso de migración hacia plataformas de código abierto, se rigen por lo establecido en la legislación vigente y se ajustan al cronograma que como anexo único forma parte de la presente Resolución.

SÉPTIMO: Las entidades desarrolladoras de programas y aplicaciones informáticas deben incrementar su producción y que sean compatibles con sistemas operativos de código abierto que respalden la implementación del proceso de migración hacia plataformas de código abierto, así como garantizar el soporte, la capacitación del personal y la comunicación a sus clientes cuando estas sean desplegadas; las que desarrollen sistemas operativos en código abierto deben garantizar la sostenibilidad y evolución de estos.

OCTAVO: Los sistemas operativos, programas y aplicaciones informáticas, previo a su despliegue, se evalúan por las entidades facultadas, y se compatibilizan con los órganos y organismos que correspondan, con el objetivo de que cumplan con los estándares de calidad y seguridad.

NOVENO: El Viceministro de Comunicaciones que atiende la Informatización, queda encargado de orientar el proceso de migración hacia plataformas de código abierto y de adoptar las medidas organizativas necesarias para cumplir lo que por la presente Resolución se dispone.

DÉCIMO: La Dirección General de Informática analiza el cumplimiento del cronograma, su implementación e impacto y propone al que suscribe, de ser necesario, las próximas acciones para continuar el desarrollo e implantación de los programas y aplicaciones de código abierto, de acuerdo con los informes semestrales que se mencionan en el apartado Tercero inciso f).

UNDÉCIMO: La Dirección General de Informática, la Dirección de Inspección y las oficinas territoriales de control del Ministerio de Comunicaciones, quedan encargadas según corresponda, del control del cumplimiento de lo que por la presente se dispone.

DISPOSICIÓN TRANSITORIA

ÚNICA: La Dirección General de Informática, elabora el procedimiento necesario para la implementación de lo dispuesto en la presente Resolución, en un plazo de sesenta días posteriores a partir de la fecha de su publicación en la Gaceta Oficial de la República de Cuba.

DISPOSICIONES FINALES

PRIMERA: Los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, adecuan y regulan para sus sistemas lo dispuesto en la presente Resolución.

SEGUNDA: La presente Resolución entra en vigor sesenta días posteriores a partir de la fecha de su publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE al Viceministro que atiende la Informatización, al Director General de Informática, a los directores de Inspección y territoriales de control, del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, y de la Oficina de Seguridad para las Redes Informáticas, y al director de Regulaciones, pertenecientes todos al Ministerio de Comunicaciones.

DÉSE CUENTA a los jefes de los órganos, organismos de la Administración Central del Estado, de la Aduana General de la República, del Instituto de Planificación Física, de la Oficina Nacional de Estadística e Información y a la Ministro Presidente del Banco Central de Cuba.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

DADA en La Habana, a los 21 días del mes de diciembre del 2020.

Jorge Luis Perdomo Di-Lella

ANEXO ÚNICO

CRONOGRAMA GENERAL DE MIGRACIÓN HACIA PLATAFORMAS DE CÓDIGO ABIERTO Y LA GENERALIZACIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS DE PRODUCCIÓN NACIONAL POR LOS ÓRGANOS, ORGANISMOS DE LA ADMINISTRACIÓN CENTRAL DEL ESTADO, EL BANCO CENTRAL DE CUBA, LA ADUANA GENERAL DE LA REPÚBLICA, EL INSTITUTO DE PLANIFICACIÓN FÍSICA Y LA OFICINA NACIONAL DE ESTADÍSTICA E INFORMACIÓN.

2021

1. Efectuar un diagnóstico, con fuerzas propias o asistidas, en todos los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, la Aduana General de la República, el Instituto de Planificación Física y la Oficina Nacional de Estadística e Información para conocer el nivel de adopción de plataformas de código abierto y programas y aplicaciones informáticas de producción nacional que poseen.

2. Evaluar las experiencias obtenidas en aquellos órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, la Aduana General de la República, el Instituto de Planificación Física y la Oficina Nacional de Estadística e Información que posean determinado nivel de adopción evidenciado durante el diagnóstico referido en el punto 1.
3. Fortalecer la gestión con el desarrollador y las entidades para que garanticen el soporte técnico a los programas y aplicaciones informáticas.
4. Realizar el proceso de formación o capacitación del personal sobre el desarrollo, implantación, administración, despliegue del soporte técnico y utilización de los programas y aplicaciones de código abierto. Por ejemplo: NOVA, OpenOffice, Navegador Firefox y Cliente de correo Thunderbird, Formato de Documento Abierto para Aplicaciones Informáticas, Open Document Format en inglés,ODF, gestor de bases de datos PostgreSQL, o sus similares.
5. Promover e impulsar el uso de programas y aplicaciones informáticas de código abierto. Por ejemplo: OpenOffice, Navegador Firefox y Cliente de correo Thunderbird, Formato de Documento Abierto para Aplicaciones Informáticas, Open Document Format en inglés, ODF, gestor de bases de datos PostgreSQL, o sus similares.
6. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, la Aduana General de la República, el Instituto de Planificación Física y la Oficina Nacional de Estadística e Información que posean infraestructuras críticas de las Tecnologías de la Información y la Comunicación, o cuya afectación tenga un impacto en la seguridad de la nación, así como aquellos que posean las condiciones para migrar hacia plataformas de código abierto, comienzan en el propio 2021.

2022 – 2023

1. Continuar el proceso de formación o capacitación del personal sobre el desarrollo, implantación, administración, despliegue, realización del soporte técnico y utilización de los programas y aplicaciones de código abierto. Por ejemplo: NOVA, OpenOffice, Navegador Firefox y Cliente de correo Thunderbird, Formato de Documento Abierto para Aplicaciones Informáticas, Open Document Format en inglés, ODF, gestor de bases de datos PostgreSQL, o sus similares.
2. Generalizar el uso de programas y aplicaciones informáticas de código abierto. Por ejemplo: OpenOffice, Navegador Firefox y Cliente de correo Thunderbird, Formato de Documento Abierto para Aplicaciones Informáticas, Open Document Format en inglés, ODF, gestor de bases de datos PostgreSQL, o sus similares.
3. Sustituir por programas y aplicaciones informáticas de código abierto, los sistemas operativos de los nodos, servidores o centros de datos privados que soportan los sistemas informáticos que estén conectados a Internet.
4. Realizar la sustitución de los sistemas operativos de las computadoras personales de escritorio y portátiles con acceso a Internet por sistemas de código abierto e incorporar programas y aplicaciones informáticas de producción nacional.

Diciembre de 2024

1. Evaluar el proceso de migración hacia plataformas de código abierto por los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, la Aduana General de la

República, el Instituto de Planificación Física y la Oficina Nacional de Estadística e Información, e informar al Viceministro que atiende la informatización del Ministerio de Comunicaciones.

RESOLUCIÓN No. 35/2020

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros de 22 de mayo de 2017, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de estos servicios y su implementación.

POR CUANTO: Debido al avance del proceso de informatización de la sociedad y el desarrollo del comercio electrónico en el país, resulta necesario establecer una normativa que regule los requerimientos mínimos a tener en cuenta en el diseño de las tiendas virtuales en la comercialización de los productos y servicios a través de las Tecnologías de la Información y la Comunicación, que se brinden mediante la modalidad de comercio electrónico.

POR TANTO: En el ejercicio de las facultades que me están conferidas, en el Artículo 145 inciso d), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar los siguientes

REQUISITOS Y FUNCIONALIDADES PARA EL DISEÑO DE TIENDAS VIRTUALES

CAPÍTULO I
Objetivos y alcance

Artículo 1. El objeto de la presente resolución es establecer los requisitos y funcionalidades mínimas a tener en cuenta en el diseño de tiendas virtuales, según las condiciones actuales de la informatización del país.

Artículo 2. Esta Resolución es de aplicación a los titulares o los representantes legales de las tiendas virtuales, en virtud de la utilización de estas para la comercialización de productos y servicios, mediante el comercio electrónico y de forma general a través de las Tecnologías de la Información y la Comunicación.

Artículo 3. La tienda virtual constituye la plataforma digital donde se exponen los bienes y servicios en oferta y su información complementaria, para que el cliente pueda realizar sus operaciones de manera totalmente autónoma.

CAPÍTULO II

Funcionalidades generales

Artículo 4. La venta en Internet de la tienda virtual se realiza a través del módulo dirigido al cliente, que le permite la realización de compras de productos y servicios.

Artículo 5. El módulo de venta en Internet de la tienda virtual debe contar con las condiciones que permitan desarrollar las funcionalidades siguientes:

a) Catálogo de productos y servicios, organizado por categorías y subcategorías en caso que se requiera, con la siguiente información de cada uno:
   I. Nombre
   II. Identificador
   III. Foto descriptiva
   IV. Precio
   V. Unidad de medida o paquete
   VI. Disponibilidad del producto
   VII. Descripción
   VIII. Manual de usuario o ficha técnica, si aplica
   IX. Tiempo estimado de entrega, si aplica
b) buscador general de productos y servicios con opciones de filtrado;
c) registro de clientes, con los datos siguientes que son solicitados al realizar compras:
   I. Nombre y apellidos
   II. Carné de identidad o documento de identificación
   III. Domicilio: con el uso de nomencladores oficialmente establecidos para el municipio y la provincia
   IV. Código postal
   V. País (solo si la tienda posee visibilidad internacional y permite la realización de compras o envíos fuera de territorio nacional)
   VI. Teléfono
   VII. Correo electrónico
   VIII. Credencial de acceso
d) selección de productos o servicios, que permite conformar una lista con los artículos a comprar y ajustar las cantidades que se quieren comprar de estos, debe permitir modificar dicha lista y realizar o cancelar la compra, muestra el precio por artículo y el total a pagar en la moneda que efectuó el pago;
e) revisión de la compra, información que se brinda al cliente para que este confirme si está de acuerdo en ejecutar la transacción y debe contener lo siguiente:
   I. Datos de la compra:
      1. Nombre del producto o servicio que se pretende comprar.
      2. Cantidad de cada producto o servicio.
      3. Precio unitario por cada producto o servicio que se pretende comprar.
      4. Subtotal por cada producto o servicio, en función de la cantidad seleccionada.

5. Total a pagar, que representa la suma del precio de cada artículo más el precio de los servicios adicionales solicitados.

II. Dirección de envío, si es diferente a la especificada en la cuenta del cliente.

III. Receptor de la compra, si es una persona diferente al cliente, caso en el cual se deben especificar los siguientes datos:

1. Nombre y apellidos del receptor en caso de ser persona natural, o nombre del establecimiento en caso de ser persona jurídica.
2. Carné de identidad o documento de identificación.
3. Domicilio: con el uso de nomencladores oficialmente establecidos para la provincia y el municipio.
4. Código postal, opcional.
5. País (solo si la tienda posee visibilidad internacional y permite la realización de compras y envíos fuera de territorio nacional).
6. Teléfono, opcional.

f) selección del método de pago, sea electrónico o en efectivo en caso que se permita pagar por el producto al ser recibido;

g) historial de compra, que muestra un seguimiento de todas las compras realizadas por el cliente con los datos siguientes:

I. Identificador de la tienda
II. Nombre del producto
III. Identificador del producto
IV. Identificador de la transacción
V. Pasarela
VI. Banco
VII. Fecha y hora de la compra
VIII. Estado actual de la compra
IX. Nombre del destinatario de la compra, que puedes ser el propio cliente
X. Domicilio del destinatario: con el uso de nomencladores para la provincia y el municipio
XI. Código postal
XII. País

Artículo 6. Además de los datos mencionados en el artículo 5, incisos a) y c), se pueden agregar otros, en dependencia del producto o servicio.

Artículo 7. El módulo de venta de la tienda virtual debe contar con los requisitos siguientes:

a) Permitir la creación de cuentas de usuarios con el objetivo de facilitar el proceso de compra a clientes, e implementar mecanismos para que estos se autentiquen mediante una credencial de acceso, la cual se almacena cifrada y cumple con la legislación vigente en la materia;
b) estar disponible en idiomas español e inglés si ofrece sus productos o servicios a personas extranjeras, y de ser requerido pueden habilitarse los recursos necesarios para el uso de otros idiomas;
c) mostrar las tasas de cambio monetario vigentes en el momento en que se realiza la compra;

d) el diseño de todas las páginas web debe ser adaptable a cualquier resolución de pantalla, este diseño adaptativo es conocido por el nombre de diseño web responsive;
e) brindar la opción a los clientes de recibir por correo electrónico o SMS los datos de las compras realizadas, notificación de transacciones bancarias y el estado de las órdenes.

CAPÍTULO III
Funcionalidades administrativas

Artículo 8. La administración de la tienda virtual se realiza a través del módulo desde el cual se controla y se establecen las relaciones entre los demás módulos de la tienda virtual.

Artículo 9. La actividad de los proveedores de la tienda virtual se realiza desde el módulo dedicado a la gestión de la disponibilidad de los productos y servicios que se ofertan en la tienda.

Artículo 10. Los módulos de administración y de proveedores de la tienda virtual cuentan con las condiciones que permitan desarrollar las funcionalidades siguientes:

a) Autenticación: se solicita al administrador o proveedor introducir su identificador y contraseña, que son validadas en una base de datos;
b) edición del catálogo: permite la gestión de los productos y los servicios, información sobre los mismos, así como la disponibilidad de estos;
c) consulta de los datos de los clientes: permite la consulta de los datos de clientes de la tienda virtual, así como de su historial de compras;
d) seguimiento de órdenes: permite a los administradores y proveedores consultar los datos de las órdenes realizadas por los clientes.

Artículo 11. La tienda virtual puede contar con otras funcionalidades, según sean requeridas por su titular o representante legal, entre las que se encuentran secciones dedicadas a preguntas más frecuentes, recomendaciones de productos nuevos o más vendidos, módulos estadísticos que faciliten el análisis del comercio, indicadores que permitan analizar los aspectos más relevantes de las tiendas, envío de noticias y espacios de intercambio para la realización de consultas.

CAPÍTULO IV
Sobre la seguridad

Artículo 12. Los módulos de la tienda virtual deben funcionar sobre conexión con transferencia segura de datos de hipertexto con protocolo HTTPS o equivalentes, de acuerdo con las normas de protección criptográfica que establece la legislación vigente.

Artículo 13. El desarrollador de la tienda virtual habilita una conexión estable y segura con el proveedor del servicio de pago a través de la infraestructura de llave pública aprobada en el país y solamente debe emplear un certificado digital que cumpla con la legislación vigente en la materia, emitido por una entidad nacional aprobada.

Artículo 14. El administrador asigna un rol de acceso a cada usuario de la tienda virtual, el cual define las funcionalidades a las que estos pueden acceder en el sistema.

Artículo 15. El representante legal de la tienda virtual es responsable de establecer la conservación de las trazas sobre las acciones realizadas en la tienda por todos los que actúan sobre esta, las cuales deben contener, si aplica, la información mínima siguiente:

a) Para las acciones realizadas por todos los actores:
   I. Credencial de usuario
   II. Acción realizada
   III. Identificador de los productos o servicios
   IV. Fecha y hora de la acción realizada
   V. Dirección IP
   VI. Dirección MAC del terminal utilizado

b) Para las acciones realizadas por los clientes se registra además:
   I. Número y banco de la tarjeta empleada
   II. Monto del pago realizado

c) Para las acciones realizadas por los otros actores se registra además:
   I. Credencial de usuario (de inferior jerarquía) sobre el cual se realizó la acción.

Artículo 16. Las trazas se conservan por un tiempo no menor a un año, en un servidor ajeno al servidor de aplicación en el cual se encuentra instalada la tienda virtual.

Artículo 17. Se solicita al cliente, en caso que se utilicen, la aceptación del uso de pequeños paquetes de datos enviados por el servidor de la tienda virtual y almacenados en el navegador con el objetivo de informar la actividad previa en este, conocidos como cookies, ya sean propias o de terceros.

Artículo 18. Todas las operaciones realizadas en la tienda virtual que impliquen el tratamiento de datos personales, cumplen con la legislación vigente en la materia.

Artículo 19. El desarrollador de la tienda virtual debe implementar los mecanismos para que el cliente exprese la aceptación de los términos y condiciones inherentes al uso de la tienda virtual, previa a la realización del pago.

Artículo 20. El titular o representante legal y el administrador de la tienda virtual son los responsables de cumplir con los requisitos de seguridad y calidad de programas y aplicaciones informáticas establecidos por la legislación vigente.

SEGUNDO: La Dirección General de Informática, la Dirección de Inspección y las oficinas territoriales de control del Ministerio de Comunicaciones, quedan encargadas según corresponda, del control del cumplimiento de lo que por la presente se dispone.

DISPOSICIÓN FINAL

ÚNICA: Esta disposición entra en vigor a los treinta días posteriores a su publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE a los presidentes del Grupo de Administración de Empresas, del Grupo Empresarial de la Informática y las Comunicaciones y de las Cadenas de Tiendas Caracol, CIMEX y Caribe.

COMUNÍQUESE a los viceministros, a los directores generales de Informática, de Comunicaciones y de la Oficina de Seguridad para las Redes Informáticas; a los directores de Regulaciones y de Inspección y a los directores territoriales de control, del Ministerio de Comunicaciones.

DÉSE CUENTA a los Ministros de Comercio Interior, de Comercio Exterior y la Inversión Extranjera, del Interior y al ministro – presidente del Banco Central de Cuba.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

ARCHÍVESE el original en la dirección Jurídica del Ministerio de Comunicaciones.

DADA en La Habana, a los 9 días del mes de marzo de 2020.

Jorge Luis Perdomo Di-Lella

RESOLUCIÓN No. 22/2020

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros, de 22 de mayo de 2017, en su numeral Diecinueve, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de disponer la asignación de los recursos de numeración, de internet y de uso conjunto a los operadores de servicios públicos de telecomunicaciones.

POR CUANTO: La Resolución 139 del Ministro de la Informática y las Comunicaciones de 6 de junio del 2008, aprueba el Registro de los Recursos de Internet de la República de Cuba que reciben las entidades autorizadas y asignan esos recursos a sus usuarios finales con acceso a Internet nacional e internacional de nuestro país; tras la aprobación de las normas regulatorias relacionadas con la informatización de la sociedad y con el objetivo de lograr un control más eficaz, se hace necesario actualizar la referida Resolución.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Establecer la inscripción de los Recursos de Internet de la República de Cuba, que reciben las entidades autorizadas y asignan esos recursos a sus usuarios finales con acceso a Internet nacional e internacional de nuestro país.

SEGUNDO: Los recursos de Internet a inscribir son los siguientes:

a) Direcciones IP: Dirección única del protocolo de Internet, asignada a cada máquina o dispositivo que se encuentra en la red.
b) Número de Sistema Autónomo o ASN: Es el número asociado a un Sistema Autónomo el cual es un grupo de redes de direcciones IP que son gestionadas por uno o más operadores de red que poseen una clara y única política de enrutamiento que se identifica por su numeración para en el intercambio de información del enrutamiento externo.
c) Sistemas de Nombres de Dominios (DNS): Es el sistema empleado en Internet para poder asignar y usar universalmente nombres unívocos para referirse a equipos, portales o sitios conectados a la Red.

TERCERO: Los Proveedores de Servicios Públicos de Acceso a Internet y Titulares de las Redes Privadas de Datos, deben inscribir en la Dirección General de Informática a través de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones sus Recursos de Internet, y acreditar su pertenencia.

CUARTO: La inscripción debe contener al menos los aspectos siguientes:

a) Datos generales de la Entidad y Responsables Administrativos y Técnicos.
b) Las asignaciones de bloques de Direcciones IP reales.
   i. Adjudicadas por LACNIC o Proveedor Público de Servicio Internet.
   ii. Adjudicadas a los Usuarios Finales.
c) Los Números de Sistemas Autónomos.
d) Los dominios asociados y servidores DNS por entidad.
   i. de tercer nivel.
   ii. de cuarto nivel.

QUINTO: Los poseedores de Recursos acreditados en la Inscripción de Recursos de Internet, están obligados a mantener actualizado su inscripción en la Dirección General de Informática a través de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, cada vez que realicen subasignaciones de los mismos, o por cambios de los datos generales de la Entidad y Responsables Administrativos y Técnicos.

SEXTO: Por los derechos de inscripción de los Recursos de Internet se abona un importe ascendente a ochenta pesos y para los trámites de actualización o renovación un importe de cuarenta pesos; el pago se hace directamente en la agencia bancaria según establece la legislación vigente del Ministerio de Finanzas y Precios y se presenta el comprobante a la Unidad Presupuestada Técnica de Control del

Espectro Radioeléctrico, quien anexa la copia al expediente.

SÉPTIMO: A los Proveedores de Servicios Públicos de Acceso a Internet y Titulares de las Redes Privadas de Datos que incumplan lo establecido en la presente Resolución, se les aplican medidas administrativas, como la notificación al responsable del órgano, organismo o institución o la invalidación temporal o definitiva de las Licencias de Operación de Red.

OCTAVO: El director General de Informática queda encargado con la elaboración de los procedimientos y formularios necesarios para la implementación de lo dispuesto en la presente Resolución en un plazo de treinta días posteriores a su publicación en la Gaceta Oficial de la República de Cuba.

NOVENO: La Dirección General de Informática del Ministerio de Comunicaciones queda encargada de la Inscripción de los Recursos de Internet de la República de Cuba y de establecer las medidas de control y supervisión para garantizar el cumplimiento de lo dispuesto en la presente Resolución.

DÉCIMO: Derogar la Resolución 139 de 6 de junio 2008, del Ministerio de la Informática y las Comunicaciones.

UNDÉCIMO: La presente Resolución entra en vigor a los treinta días posteriores a su fecha de publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE al director general de Informática y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros y al director de Regulaciones del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

Dada en La Habana, a los días 10 del mes de febrero del 2020.

Jorge Luis Perdomo Di-Lella

RESOLUCIÓN No. 80/2019

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros, de 22 de mayo de 2017, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales,

nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de estos.

POR CUANTO: Resulta necesario modificar la velocidad considerada como banda ancha para los servicios de datos en el país, acorde a las realidades actuales y consecuentemente actualizar la Resolución 319 del Ministro de Comunicaciones, de 23 de diciembre de 2015.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el Artículo 100, inciso a), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Establecer que la velocidad que es considerada como banda ancha es aquella cuyo valor es igual o superior a las establecidas a continuación:

Velocidad de bajada	Velocidad de subida
1Mbps	256kbps

SEGUNDO: Disponer que a partir de la entrada en vigor de la presente Resolución, toda información estadística relacionada con los abonados de Internet de banda ancha tenga en cuenta lo establecido en el apartado Primero de la presente normativa.

TERCERO: Derogar la Resolución 319 del Ministro de Comunicaciones, de 23 de diciembre de 2015.

NOTÍFÍQUESE a la Presidenta Ejecutiva de la Empresa de Telecomunicaciones de Cuba S.A.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, Informática; Organización, Planificación e Información y de la Oficina de Seguridad para las Redes Informáticas, a los directores de Regulaciones, Inspección y de las oficinas Territoriales de Control, pertenecientes todos al Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 3 días del mes de abril de 2019.

Jorge Luis Perdomo Di-Lella

RESOLUCIÓN No. 74/2018

POR CUANTO: El Acuerdo No. 8151 del Consejo de Ministros, de 22 de mayo de 2017, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de estos.

POR CUANTO: En aras de avanzar gradualmente en la ampliación y desarrollo de los servicios de telecomunicaciones y de las tecnologías de la información y la comunicación en el país; se requiere el desarrollo de la infraestructura nacional de telecomunicaciones, con el objetivo de satisfacer la creciente demanda de acceso a estos, por lo que resulta necesario reglamentar el ámbito de actuación del proveedor de infraestructuras de telecomunicaciones.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el Artículo 100, inciso a) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO SOBRE LOS PROVEEDORES DE INFRAESTRUCTURAS DE TELECOMUNICACIONES

CAPÍTULO I
OBJETO, GENERALIDADES Y LEGISLACIÓN APLICABLE

Artículo 1. El objeto del presente Reglamento es el establecimiento de las normas para la organización, funcionamiento, y expedición de licencias de operación de los proveedores de infraestructura de telecomunicaciones, en lo adelante el proveedor.

Artículo 2. A los efectos del presente Reglamento, los términos que se citan a continuación tienen el significado siguiente:

a) Infraestructura de telecomunicaciones: se consideran como tal las infraestructuras pasivas de telecomunicaciones y las redes de telecomunicaciones.
b) Infraestructura pasiva de telecomunicaciones: aquellas instalaciones aéreas, terrestres, subterráneas, submarinas o subacuáticas, compuestas principalmente por torres, mástiles, postes, ductos, canales, conductos, cámaras, cables, fibra oscura, entre otros; que permiten el uso de los componentes activos de la red necesarios para la transmisión y recepción de señales y que son utilizados para proveer soporte a redes y servicios de telecomunicaciones.
c) Operador de redes de telecomunicaciones: persona jurídica que se le otorga un título habilitante de acuerdo con la legislación vigente para la instalación, operación, explotación, mantenimiento

y comercialización de redes de telecomunicaciones para ofrecer servicios públicos de telecomunicaciones a usuarios finales.

d) Red de telecomunicación: conjunto de facilidades que proporcionan conexiones entre dos o más puntos definidos, para facilitar la telecomunicación entre ellos y que pueden estar constituidos por canales de transmisión, circuitos, dispositivos, equipos terminales y centrales de conmutación.
e) Red privada de telecomunicaciones: red de telecomunicaciones cuya infraestructura de red está instalada en una o en distintas localidades geográficas e interconectadas entre sí por enlaces de telecomunicaciones con el objetivo de satisfacer las necesidades internas de servicios de telecomunicaciones de su titular.
f) Red pública de telecomunicaciones: red de telecomunicaciones que se explota principalmente para prestar servicios públicos de telecomunicaciones y tecnologías de la información y la comunicación.
g) Servicio público de telecomunicaciones: aquel destinado a satisfacer las necesidades del público en general, sin distinción de persona natural o jurídica, que se presta a través de redes expresamente autorizadas para ello, que permiten el acceso de los usuarios a las telecomunicaciones y a las tecnologías de la información y la comunicación.

Artículo 3. El proveedor de infraestructuras de telecomunicaciones es la persona jurídica autorizada a:

a) Instalar, adquirir, operar, comercializar y mantener infraestructuras pasivas de telecomunicaciones propias o de terceros.
b) Instalar, adquirir, comercializar, mantener y gestionar el uso de las redes de telecomunicaciones propias o de terceros, para proporcionar facilidades de red a operadores de redes de telecomunicaciones, a proveedores de servicios públicos y a redes privadas de telecomunicaciones.

Artículo 4. Las redes privadas de telecomunicaciones pueden utilizar infraestructuras provistas por un proveedor de infraestructura de telecomunicaciones para su operación, de conformidad con las disposiciones del presente Reglamento.

CAPÍTULO II
DEL OTORGAMIENTO, RENOVACIÓN Y CANCELACIÓN DE LAS LICENCIAS

Artículo 5.1. Las personas jurídicas solicitan la licencia para proveer infraestructuras de telecomunicaciones que emite la dirección general de Comunicaciones, en lo adelante DGC, del Ministerio de Comunicaciones.

2. Se exceptúan de solicitar la licencia referida en el párrafo anterior, las entidades del Ministerio de las Fuerzas Armadas Revolucionarias o del Ministerio del Interior que provean infraestructuras de telecomunicaciones a los órganos de la Defensa, Seguridad y Orden Interior y a otros que se aprueben por el Ministerio de Comunicaciones. En los casos, que brinden estos servicios a terceros, deben cumplir lo regulado por el presente Reglamento.

Artículo 6. La DGC a través de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, en lo adelante UPTCER se encarga de la recepción, análisis y tramitación de las solicitudes de licencias.

Artículo 7.1. Para solicitar la licencia se suministra la información siguiente:

a) Datos generales de la persona jurídica solicitante y de su representante legal además de la disposición normativa o poder que lo faculta para ello;
b) datos de la zona de servicio y de la ubicación de las infraestructuras pasivas y las redes instaladas hasta la fecha de solicitada la licencia;
c) datos técnicos de la infraestructura pasiva o de red instalada hasta la fecha de solicitada la licencia, donde se detalle:

i infraestructura y arquitectura de la red;
ii alcance geográfico;
iii equipamiento técnico;
iv plataformas y programas informáticos que utilice; y
v datos de equipamiento y puntos de conexión que se utilicen.

d) otros documentos de interés que se soliciten por la UPTCER como requisito adicional a lo regulado por el presente Reglamento.

2. Los datos a declarar por los solicitantes, que estén relacionados con infraestructuras de los órganos de la Defensa, la Seguridad y el Orden Interior se informan según estos lo determinen.

Artículo 8. Los datos declarados pueden ser objeto de comprobación por los inspectores de la Oficina Territorial de Control, en lo adelante OTC del Ministerio de Comunicaciones.

Artículo 9.1. La DGC revisa las solicitudes y dispone de treinta (30) días hábiles para emitir o denegar las licencias.

2. Los proveedores a los que les sean otorgadas las licencias son inscritos por la DGC en el Control Administrativo Central Interno y se publica en el sitio web institucional del Ministerio de Comunicaciones, la relación de estos.

Artículo 10. La licencia de operación se concede al proveedor por un plazo de diez (10) años, el que puede ser prorrogado a solicitud de su titular.

Artículo 11. La modificación de lo dispuesto en el inciso a) del artículo 7 conlleva a la renovación de la licencia, por lo que el proveedor comunica a la UPTCER en un plazo de treinta (30) días posteriores a su ocurrencia.

Artículo 12. El proveedor informa a la UPTCER con una antelación no inferior a los sesenta (60) días previos al inicio de la instalación de nuevas infraestructuras de telecomunicaciones propias, la información relativa a estas según lo dispuesto en los incisos b), c) y d) del artículo 7, para ser actualizada en el Control Administrativo Central Interno del Ministerio de Comunicaciones.

Artículo 13. El proveedor, noventa (90) días antes del vencimiento del plazo de vigencia de la licencia de operación, presenta a la UPTCER la solicitud de su renovación. De no tramitarse en el término establecido dicha solicitud, la licencia se cancela de oficio y el proveedor debe efectuar los trámites para una nueva licencia.

Artículo 14. Constituyen causas de cancelación de la licencia de operación por parte de la UPTCER las siguientes:

a) La invalidez de la licencia de operación por los inspectores de la OTC, cuando se incumpla lo dispuesto en el presente Reglamento;
b) la renuncia presentada por escrito ante la UPTCER por parte del proveedor;
c) la cesión o gravamen, en todo o en parte, a favor de tercero, de los derechos que son objeto de la licencia otorgada; y
d) las demás que correspondan según la legislación vigente.

Artículo 15. Los proveedores abonan la cantidad de quinientos pesos cubanos (500.00 CUP) por el otorgamiento de la licencia, y para los trámites de su renovación, cien pesos cubanos (100.00 CUP). Estos pagos se realizan en la sucursal bancaria según establece la legislación vigente del Ministerio de Finanzas y Precios y la copia del comprobante se presenta en la UPTCER, quien lo anexa al expediente.

CAPÍTULO III
DE LOS DEBERES DE LOS PROVEEDORES

Artículo 16. Los proveedores de infraestructura de telecomunicaciones tienen los deberes siguientes:

a) Ofrecer su infraestructura de telecomunicaciones según las tarifas establecidas en materia de formación y aprobación de precios;
b) observar las disposiciones normativas vigentes en el país y cumplir los principios siguientes:

    i Igualdad de Acceso: el proveedor debe conectar las redes o los servicios en condiciones equivalentes para todos los operadores de redes de telecomunicaciones.
    ii Neutralidad: el proveedor que posea derechos exclusivos o una posición predominante en el mercado o condiciones particulares que le beneficien, está obligado a no utilizar estas situaciones para prestar servicios de telecomunicaciones en condiciones de mayor ventaja para sí mismo y en detrimento de otros operadores o proveedores.
    iii No Discriminación: el proveedor no debe dar un trato diferenciado a operadores y proveedores, que busquen o pretendan favorecer a éstos o a sí mismos, en detrimento de cualquiera de los otros operadores de redes de telecomunicaciones existentes.

iv Transparencia: el proveedor está obligado a poner en conocimiento de los restantes proveedores las condiciones técnicas y comerciales, bajo la aplicación de cláusulas de confidencialidad.

c) no utilizar el control de su infraestructura de telecomunicaciones, en detrimento de la posición de otros proveedores de servicios de infraestructura de telecomunicaciones u operadores de redes y proveedores de servicios de telecomunicaciones autorizados en el país;
d) emplear medidas de seguridad destinadas a salvaguardar y proteger el secreto y la inviolabilidad de las comunicaciones y la protección y adecuado tratamiento de los datos personales de sus clientes;
e) adoptar medidas de seguridad destinadas a proteger las redes de telecomunicaciones que se soportan sobre su infraestructura pasiva de telecomunicaciones;
f) garantizar que no se afecte la prestación de otros servicios, ni se generen daños a la infraestructura de uso público ni a la de terceros;
g) no introducir, ejecutar, distribuir o conservar en los medios de cómputo, programas y contenidos que puedan afectar la integridad y seguridad del país, así como información contraria al interés social, la moral y las buenas costumbres;
h) acatar las disposiciones establecidas por los órganos de la Defensa del país ante situaciones excepcionales, así como para la realización de tareas impostergables para el aseguramiento de la Defensa, la Seguridad y el Orden Interior;
i) compatibilizar con las autoridades competentes el empleo de medidas, métodos, mecanismos o dispositivos criptográficos;
j) poseer un Plan de Contingencia actualizado para la mitigación del impacto de los riesgos;
k) observar las normativas vigentes en materia de salud pública, medio ambiente, seguridad nacional y orden interior;
l) poseer la base de datos que contenga la información referente al mapeo de su infraestructura;
m) informar a sus usuarios con sesenta (60) días de antelación como mínimo, los cambios técnicos, en la zona de servicio o en la ubicación de las infraestructuras pasivas o de sus redes de telecomunicaciones que afecten sus servicios, salvo que las partes pactaran otro término en sus relaciones contractuales;
n) mantener la provisión de las infraestructuras pasivas o de las redes de telecomunicaciones, aunque existan discrepancias con sus clientes hasta tanto sean resueltas por la DGC;
o) brindar las informaciones solicitadas por el Ministerio de Comunicaciones según la periodicidad que se determine por este; y
p) los que se deriven del presente Reglamento y demás disposiciones jurídicas vigentes en materia de telecomunicaciones.

Artículo 17. Los proveedores que empleen equipos de telecomunicaciones y tecnologías de la información y la comunicación y se conecten a redes públicas de telecomunicaciones o que hagan uso del espectro radioeléctrico, tienen que haber obtenido previamente el correspondiente Certificado de Homologación para estos, según lo establecido en las normativas vigentes.

Artículo 18. En caso de discrepancias entre los proveedores de infraestructuras y sus clientes, la DGC dispone de un plazo de treinta (30) días para emitir su decisión a partir de la fecha en que se le notifique oficialmente por una de las partes.

CAPÍTULO IV
DE LOS INCUMPLIMIENTOS

Artículo 19. El proveedor que incumpla las condiciones específicas de la licencia otorgada o de lo dispuesto en el presente Reglamento está sujeto a la aplicación de las medidas siguientes:

a) Notificación preventiva del incumplimiento detectado al proveedor controlado y envío de copia al jefe del órgano, organismo de la Administración Central del Estado o entidad a la que se subordina o adscribe, o por el que es atendido o patrocinado;
b) suspensión temporal hasta dos (2) años de la licencia de operación concedida al proveedor;
c) cancelación de la licencia de operación concedida al proveedor; y.
d) otras medidas que correspondan de conformidad con el marco jurídico establecido en el país.

Artículo 20. El inspector del Ministerio de Comunicaciones es la autoridad facultada para aplicar las medidas referidas en el artículo anterior e informar a la UPTCER sobre la medida impuesta y la decisión acerca de su aplicación.

Artículo 21. Cuando las medidas aplicadas sean las de suspensión temporal o cancelación de las licencias de operación, se le concede un plazo de sesenta (60) días al proveedor para notificar a sus clientes la fecha de cesación de sus servicios, una vez transcurrido dicho plazo se ejecutan las medidas correspondientes y comienza el cese temporal o definitivo de estos.

Artículo 22. En el caso de que la cancelación de la licencia, incluya la medida accesoria de confiscación de la infraestructura de telecomunicaciones propia y los equipos del proveedor puede tramitarse por el Ministerio de Comunicaciones, la transmisión de la propiedad de estos a otros proveedores de infraestructura de telecomunicaciones o a operadores de redes de telecomunicaciones, con la finalidad de asegurar la continuidad y eficaz prestación de los servicios.

Artículo 23. Todo proveedor sujeto a la aplicación de las medidas descritas anteriormente, puede apelar en primera instancia, a través de la UPTCER, ante el director general de Comunicaciones, en un plazo de diez (10) días hábiles contados a partir de la fecha de impuesta la medida, presentar las alegaciones y aportar las pruebas que crea; el cual dispone de treinta (30) días hábiles para dar respuesta a esta, contados a partir de la fecha en que haya sido recibida la apelación.

Artículo 24. El proveedor que desee impugnar la decisión de la primera instancia de apelación, lo solicita a través de la UPTCER, en un plazo de diez (10) días hábiles siguientes a su notificación, a partir de las alegaciones y la aportación de otras pruebas que crea convenientes no presentadas en la apelación, el que suscribe dispone de sesenta (60) días hábiles para dar respuesta a esta, contados a partir de la fecha en que haya sido recibida; contra lo resuelto en esta instancia no cabe otro recurso en la vía administrativa y queda expedita la vía judicial.

Artículo 25. El proveedor que ha sido objeto de una medida que motive la cancelación de la licencia de operación puede, resueltas las causas que dieron lugar a la medida impuesta, volver a presentar a la DGC a través de la UPTCER su solicitud de licencia siempre que hayan transcurrido seis (6) meses como mínimo de la imposición de esta; el director general de Comunicaciones tiene en cuenta la información presentada y comprobada por los inspectores de la OTC, así como la solución de las deficiencias detectadas y decide sobre la nueva inscripción.

SEGUNDO: El proveedor antes de satisfacer cualquier demanda de instalación o utilización de las infraestructuras de telecomunicaciones por operadores de redes, proveedores de servicios o titulares de redes privadas de telecomunicaciones, solicita la presentación de las autorizaciones correspondientes expedidas por el Ministerio de Comunicaciones.

TERCERO: El director general de Comunicaciones queda responsabilizado con la elaboración del procedimiento interno aplicable a las unidades organizativas del Ministerio de Comunicaciones para la implementación de lo dispuesto en la presente, en un plazo de sesenta (60) días a partir de la fecha de su publicación en la Gaceta Oficial de la República de Cuba.

CUARTO: Los directores generales de Comunicaciones y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, el director de Inspección y los directores territoriales de control del Ministerio de Comunicaciones, son responsables de controlar el cumplimiento de lo dispuesto en la presente Resolución, según corresponda.

DISPOSICIÓN TRANSITORIA

ÚNICA: Toda persona jurídica que realice los servicios relacionados en el artículo 3 del presente Reglamento, posee un plazo de sesenta (60) días contados a partir de la fecha de entrada en vigor de la presente Resolución para solicitar la licencia de proveedor de infraestructura de telecomunicaciones.

DISPOSICIÓN FINAL

ÚNICA: La presente Resolución entra en vigor a los sesenta (60) días posteriores a su fecha de publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE a los directores generales de Comunicaciones y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, al director de Inspección, al Presidente del Grupo Empresarial de la Informática y las Comunicaciones y a los directores territoriales de control.

COMUNÍQUESE a los viceministros, a los directores generales de Informática y de la Oficina de Seguridad para las Redes Informáticas, al director de Regulaciones, todos pertenecientes al Ministerio de Comunicaciones y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A.

ARCHÍVESE el original en la dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 26 días del mes de marzo de 2018.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 121/2017

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en su numeral Tercero del Apartado Primero, establece que el Ministerio de Comunicaciones es el organismo encargado de proponer, y una vez aprobada, ejecutar y controlar la política sobre el uso del ciberespacio, así como planificar, implementar, reglamentar, administrar y controlar el sistema de medidas necesarias para su defensa y realizar las coordinaciones internacionales requeridas a ese fin.

POR CUANTO: La Resolución No. 127 del ministro de Comunicaciones, de fecha 24 de julio de 2007, aprobó y puso en vigor el "Reglamento de Seguridad para las Tecnologías de la Información", en el que se establece que en todas las redes informáticas se tienen que implementar mecanismos de seguridad de forma tal que se garantice la protección de las mismas, por lo que resulta procedente establecer las medidas básicas para configurar los servidores de correo electrónico de las redes de datos del país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el inciso a), del Artículo 100 de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Establecer las medidas básicas para configurar los servidores de correo electrónico que se deben implementar en las redes de datos del país debidamente autorizadas, en lo adelante las redes, las cuales se refieren a continuación:

1. Control de acceso a los puertos 25, 443 y 587 en entrada/salida.
2. Implementación de reglas anti-relay (protección contra correos no solicitados).
3. Control de resolución inversa.
4. Política de trazas de auditoría.
5. Número máximo de destinatarios en una transacción SMTP (Simple Mail Transfer Protocol en inglés – protocolo para la transferencia simple de correo en español).
6. Tamaño máximo de mensaje.
7. Definición de registros SPF (*Sender Policy Framework en inglés- convenio de remitentes en español)*.
8. Chequeo de registro SPF en el flujo de entrada.
9. Control de destinatarios existentes.

10. Control de flujo SMTP.
11. Sincronización de tiempo.
12. Acceso cifrado.
13. Servicio Antivirus.
14. Autenticación.
15. Servicio de cambio de contraseña.
16. Servicio antispam (método para prevenir el correo basura).

Las aclaraciones requeridas relacionadas con la implementación de las medidas básicas para configurar los servidores de correo electrónico, se establecen en el Anexo Único de la presente Resolución como parte integrante de la misma.

SEGUNDO: El titular o representante legal de la red de datos es responsable por la implementación en sus redes, de las medidas básicas que por la presente se establecen para configurar los servidores de correo electrónico.

TERCERO: A los efectos de la presente, los términos que se relacionan tienen el significado siguiente:

1. **Ataque informático:** Intento de acceso o acceso a una red informática mediante la explotación de vulnerabilidades existentes en su seguridad.
2. **Riesgo informático:** Probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en las redes.
3. **Red de datos:** Red de telecomunicaciones cuya infraestructura de red está instalada en una misma localidad o en distintas localidades geográficas e interconectadas entre sí por enlaces de telecomunicaciones públicos y propios, que satisface las necesidades de transmisión de datos de su titular.
4. **Resolución inversa de IP:** Proceso en que a partir de la dirección IP de un dispositivo, se intenta llegar al nombre asociado a este.
5. **Sistemas de Nombres de Dominios (DNS):** Es el sistema empleado en Internet para asignar y usar universalmente nombres unívocos para referirse a equipos, portales o sitios conectados a la Red.
6. **Servidor de nivel base**: Servidor que presta el servicio de correo electrónico y almacena los buzones de los usuarios de una red.
7. **Servidor de primer nivel**: Servidor encargado de recibir todo el correo electrónico destinado a un grupo de dominios y distribuirlo a cada uno de los subdominios, de igual manera reciben el correo procedente de los subdominios y lo reenvían a los destinatarios finales.
8. **Vulnerabilidad informática:** Aspecto de la aplicación que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático y califica su nivel de riesgo.

CUARTO: Los directores de las oficinas territoriales de control, el director de Inspección, el director general de la Oficina de Seguridad para las Redes Informáticas y el director general de Informática del Ministerio de Comunicaciones, quedan encargados de instrumentar las medidas para el control y fiscalización de lo dispuesto en la presente Resolución.

QUINTO: Los titulares de las redes privadas de los órganos de la Defensa, se exceptúan del cumplimiento de lo establecido en la presente Resolución, y quedan sujetos a lo dispuesto en sus normas jurídicas.

SEXTO: La presente Resolución entra en vigor a los noventa (90) días posteriores a la fecha de su publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE a los directores generales de Informática y de la Oficina de Seguridad para las Redes Informáticas, a los directores territoriales de control y al director de Inspección, todos pertenecientes al Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, al director general de Comunicaciones, al director de Regulaciones y al director del Centro de Comunicaciones, todos pertenecientes al Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 5 días del mes de abril de 2017.

Maimir Mesa Ramos
Ministro

Anexo
Resolución No. 121/2017

ACLARACIONES DE LAS MEDIDAS BÁSICAS PARA CONFIGURAR LOS SERVIDORES DE CORREO ELECTRÓNICO.

1. Control de acceso a los puertos 25, 443 y 587 en entrada/salida.

   El puerto virtual 25 SMTP controla el acceso para el tráfico tanto de llegada como de salida. El puerto virtual 443 controla el tráfico de información sensible HTTPS (protocolo seguro de transferencia de hipertextos) utilizando cifrado basado en SSL (capa de puertos seguros) o TLS (seguridad en la capa de transporte) para los usuarios y claves. El puerto virtual 587 controla el acceso para SMTP autenticado sobre SSL o sobre TLS. El uso de los puertos 443 y 587 antes mencionados son los recomendados por medidas de seguridad, u otro que se asigne siempre que sea cifrado. La cantidad de servidores que pueden enviar o recibir correo debe limitarse, en correspondencia con las necesidades reales de cada entidad y bajo el principio de la racionalidad. Las computadoras conectadas a la red que utilizan el servicio deben ser configuradas para que reciban/envíen correos electrónicos únicamente a través del servidor establecido en cada entidad.

2. Implementación de reglas Anti-Relay.

   La adopción de medidas anti-relay se considera uno de los pasos básicos para la puesta en marcha de un servicio de correo. De no cumplirse este criterio se corre el riesgo de publicación en múltiples repositorios en Internet, por configuración inadecuada del servicio, para que sea utilizado para el envío de spam.

   Por lo anterior, el servicio de correo solo se brinda para la red predeterminada. La dirección IP para este servicio está claramente definida y solo estas direcciones tienen privilegios concedidos para usar el correo. Lo anterior implica que las direcciones IP de cada red, una vez definidas, pueden establecer conexión SMTP hacia el servidor, aceptando mensajes cuyo destino sea la propia red o dominios delegados[1].

3. Control de resolución inversa.

   Debe definirse la resolución inversa de las direcciones IP asignadas al servicio de correo de primer nivel, encargadas del encaminamiento de entrada y salida de cada red[2].

4. Política de trazas de auditoría.

   Deben almacenarse y conservarse en cada red los ficheros de trazas (logs en inglés) de acuerdo con la legislación vigente, de forma que las mismas permitan la identificación de posibles problemas o incidentes y sirvan como fuente de datos para estudios estadísticos; deben contener al menos los datos siguientes: fecha y hora de la transacción, nombres de los servidores que reciben/envían, identificador (ID) del mensaje, dirección de origen/destino, nombre del servidor que actúa como relay de correo, el estado de la transacción y el tamaño del mensaje.

5. Número máximo de destinatarios en una transacción SMTP.

   Los servidores de correo electrónico deben configurarse para aceptar transacciones con un máximo de 100 destinatarios (RCPT TO)[3] en una sola conexión SMTP. Deben adoptarse las medidas técnicas necesarias para que se bloqueen las transacciones SMTP con más de 100 destinatarios. Los límites (mínimo y máximo) de destinatarios en una sola conexión SMTP deben ser definidos y aprobados por la máxima dirección de cada red privada, en dependencia de los recursos técnicos disponibles.

6. Tamaño máximo de mensaje.

[1] RFC2505/RFC2635.
[2] RFC3172.
RFC (request for comments en inglés) (Petición de comentarios en español) publicaciones del grupo de trabajo de ingeniería de internet (IETF) relacionados con protocolos, procedimientos etc.
[3] RFC2821.

El tamaño máximo del mensaje debe ser controlado, formando parte de la configuración de los servidores de primer nivel. El tamaño máximo del mensaje debe ser definido en cada institución atendiendo a sus propias características.

7. Definición de registros SPF.

Debe definirse en cada red su zona del Sistema de Nombres de Dominio (DNS en inglés) los registros SPF (*Sender Policy Framework- convenio de remitentes en español)* de todos los dominios bajo su responsabilidad, asociándolos a los nodos de correo que efectúen el encaminamiento de salida SMTP (servidores de primer nivel)[4].

Esto posibilita que se ponga a disposición de todos los servidores de correo con los que se intercambia mensajería la relación de servidores autorizados a estos fines. Lo anterior disminuye la probabilidad de materialización de posibles ataques y/o el aumento de la carga en el servicio por mensajes devueltos.

8. Chequeo de registro SPF en el flujo de entrada.

Deben configurarse en cada red los servidores de primer nivel para que se lleven a cabo los correspondientes chequeos SPF del correo entrante. Este criterio establece en todo caso la posibilidad de analizar los mensajes entrantes a la red para determinar si se cumplen los registros SPF publicados por el responsable del dominio. Deben establecerse de igual forma las acciones a ejecutar ante los mensajes que no superen el test aplicado.

9. Control de destinatarios existentes.

Deben aplicarse en cada red los mecanismos de rechazo en los servidores de nivel base para los mensajes dirigidos a destinatarios no existentes.

10. Control de flujo SMTP.

Debe disponerse en cada red de mecanismos de control de flujo en las transacciones SMTP internas y externas. Estos mecanismos permiten controlar el número de correos enviados por una IP en un intervalo de tiempo determinado.

11. Sincronización de tiempo.

En el servicio de correo electrónico se configura correctamente la zona horaria y deben sincronizarse todos los servidores de correo electrónico de las organizaciones tanto de primer nivel como nodos intermedios y servidores de almacenamiento[5] con un servidor de la propia red u otro que ofrezca el servicio, se puede utilizar NTP *(Network Time Protocol en inglés - protocolo de red de tiempo en español*).

[4] RFC4408.
[5] RFC3172/ RFC4330.

12. Acceso cifrado.

Debe considerarse en cada red ofrecer el servicio basado en protocolos de recogida de mensajes con cifrado SSL/TLS[6] (POPs, IMAPs)[7] y un servicio de correo saliente SMTP con TLS, así como acceso al correo por Web vía HTTPs para los usuarios externos. Debiendo tramitar la aprobación, de conformidad con la legislación vigente, acerca de la utilización de cualquier tipo de aplicación o servicio soportado que implique el cifrado de la información.

13. Servicio Antivirus.

Debe disponerse en cada red de un servicio antivirus que analice tanto los mensajes entrantes como los salientes en los servidores de correo. De igual forma, se deben establecer las acciones a ejecutar en cada caso detectado (eliminación del adjunto infectado sustituyéndolo por un aviso, puesta en cuarentena del mensaje completo, eliminación, aviso al remitente, entre otras).

14. Autenticación.

Debe implementarse en cada red la autenticación con el fin de elevar los niveles de seguridad y eficacia del servicio de correo electrónico, prevenir la fuga de datos, así como de disminuir la posibilidad de que su dominio sea utilizado como "puente" para el envío de correos masivos, puede implementarse SMTP.

15. Servicio de cambio de contraseña.

El servicio debe ofrecer al usuario la posibilidad de cambiar su contraseña, de forma autónoma e inmediata, sin intervención de un tercero y con el objetivo de garantizar la privacidad de la misma. De igual forma debe exigir los requisitos para la utilización de contraseñas como método de autenticación establecidos en la legislación vigente.

16. Servicio antispam.

Debe disponerse en cada red de un servicio antispam que analice los mensajes entrantes y actúe sobre aquellos que considere spam según la política interna establecida y su correspondencia con la legislación vigente al respecto.

[6] SSL/TLS protocolos para establecer comunicaciones seguras usando certificados digitales.
[7] POPs, IMAPs protocolos de internet que permiten el acceso a cuentas de correo de su espacio WEB.

RESOLUCIÓN No. 181/2016

POR CUANTO: El Acuerdo No. 7380, de fecha 28 de febrero del 2013, adoptado por el Consejo de Ministros, en el numeral Cuarto, Apartado Primero establece que el Ministerio de Comunicaciones tiene como función específica la de ordenar, regular, y controlar los servicios de telecomunicaciones, radiocomunicaciones informáticos y postales, nacionales e internacionales la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos.

POR CUANTO: El Acuerdo No. 7939 del Consejo de Ministros, de fecha 22 de junio de 2016; establece mecanismos de coordinación y acciones que contribuyan a la implantación del Protocolo IPv6 a nivel nacional, encarga al Ministro de Comunicaciones con la introducción paulatina de este, y dispuso que los ministros de Educación y Educación Superior son responsables de implementar la preparación de los estudiantes sobre el estudio en todos los niveles educativos del Protocolo IPv6; por lo que se hace necesario aprobar una nueva metodología para la preparación progresiva de la Introducción del protocolo IPv6 en las redes de datos, sistemas y aplicaciones informáticas del país, que actualice y atempere a las realidades actuales el contenido normativo de la Resolución No. 156 del Ministro de la Informática y las Comunicaciones, de fecha 14 de agosto de 2008 emitida con similares objetivos y en consecuencia proceder a su derogación.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas por el Artículo 100 inciso a), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar la siguiente:

METODOLOGÍA PARA LA PREPARACIÓN PROGRESIVA DE LA INTRODUCCIÓN DEL PROTOCOLO IPv6 EN LAS REDES DE DATOS, SISTEMAS Y APLICACIONES INFORMÁTICAS DEL PAÍS

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1: La presente metodología constituye la base para la preparación progresiva para la introducción del protocolo IPv6, la cual precisa las etapas y tareas que deben contemplar las personas jurídicas que son titulares de redes de datos públicas y privadas en el territorio nacional, organizadas y coordinadas a través de los órganos, organismos y organizaciones; a los que se les subordinan o adscriben, o por los que son atendidos o patrocinados, en lo adelante entidades coordinadoras, durante el periodo que dure la introducción al nuevo protocolo IPv6.

Artículo 2: La Introducción consta de tareas a desarrollar en los próximos años, que se ajustan a las necesidades que requiere satisfacer el país, para introducir el protocolo IPv6 y la coexistencia de las redes que soportan tanto IPv4 como IPv6.

Artículo 3: A los efectos de la presente metodología, los términos que se citan a continuación tienen el significado siguiente:

a) **IP:** protocolo de Internet.
b) **Nombres de dominio:** nombre que se utiliza para identificar recursos en una Red (una terminal o varias terminales en Red o un sitio en Internet), que facilitan la memorización de las direcciones. Los dominios constan de nombres separados por punto (.)
c) **Protocolo:** conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen comprensiblemente entre ellos para transmitir información**.** Es un término de comunicaciones y su función es fijar reglas de funcionamiento, a todos los niveles, a las que han de atenerse los distintos sistemas informáticos para poder comprenderse.
d) **Protocolo IPv6 nativo:** protocolo IP versión 6 puro, sin emplear métodos de transición.
e) **Sistema de nombres de dominio (DNS):** es la base de datos distribuida en donde los nombres de dominio son asociados a determinados recursos de Internet (por ejemplo direcciones IP). Los datos del DNS están distribuidos en varios servidores de nombres y responde a una arquitectura cliente-servidor y obedece a una estructura jerárquica.

CAPÍTULO II
DE LAS ETAPAS

Artículo 4: Las etapas que componen la metodología, por orden de ejecución son las siguientes:

a) Preparación del personal;
b) levantamiento de información;
c) proyección de trabajo;
d) análisis de presupuesto; y
e) desarrollo de proyectos de pruebas piloto IPv6.

Artículo 5: Las tareas están previstas para realizarse en veinticuatro (24) meses a partir de la entrada en vigor de la presente Resolución.

SECCIÓN I
Preparación del personal

Artículo 6: La etapa de preparación del personal está compuesta por las tareas siguientes:

a) Designar al personal técnico especializado y su responsable, los que deben estar dirigidos por un funcionario que se establezca al efecto por el jefe máximo de cada entidad coordinadora.
b) El responsable y el personal técnico especializado designado de cada entidad coordinadora organizan el trabajo a realizar por los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben; o los que atienden o patrocinan, en su esfera de acción.
c) El personal técnico designado de cada entidad coordinadora recibe preparación técnica y metodológica, que les permita realizar la identificación e inventario de los sistemas informáticos,

aplicaciones y los elementos activos de las redes, así como trabajar con protocolo IP, cualesquiera que estos sean.

d) El personal técnico designado de cada entidad coordinadora en el término de doce (12) meses debe desarrollar cursos de capacitación sobre el nuevo protocolo IPv6, para impartirlo al personal técnico de los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben, o los que atienden o patrocinan.

SECCIÓN II
Levantamiento de información

Artículo 7: La etapa de levantamiento de información está compuesta por las tareas siguientes:

a) El personal técnico de cada entidad coordinadora organiza el levantamiento a realizar por los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben, o los que atienden o patrocinan; consistente en identificar e inventariar sistemas informáticos, aplicaciones, servicios y los elementos activos de cualquiera de las redes, que no están aptos para el trabajo con los dos protocolos IPv4 e IPv6, por lo que requieren ser cambiados y los que se determine que no tienen que variar aunque utilicen protocolo IP.

b) El responsable del personal técnico especializado de cada entidad coordinadora consolida la información del inventario realizado por los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben, o los que atienden o patrocinan.

SECCIÓN III
Proyección de trabajo

Artículo 8: La etapa de proyección de trabajo está compuesta por las tareas siguientes:

a) El personal técnico capacitado como consecuencia de las revisiones previstas anteriormente y de la identificación de todos los equipos, sistemas, aplicaciones informáticas y servicios que deben ser cambiados, elabora los planes de trabajo específicos para realizar los cambios necesarios de forma escalonada en el tiempo, la modificación a los planes de contingencias y los planes de direccionamiento para la red con direcciones IPv6. Estos planes deben ser chequeados y actualizados periódicamente por el personal técnico especializado correspondiente, haciendo énfasis en los temas relacionados con la seguridad.

b) Los productores de aplicaciones como parte de sus planes específicos, deben evaluar el rediseño y la puesta en explotación de las aplicaciones por estos desarrolladas, que resulten sensibles al cambio de protocolo y que funcionan en el país, para que estas sean compatibles con IPv6; y tener en cuenta que las nuevas aplicaciones que se relacionen con protocolo IP deben ser desarrolladas con compatibilidad con IPv6. Estos planes deben ser chequeados y actualizados periódicamente entre el personal técnico especializado de cada entidad coordinadora con los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben, o los que atienden o patrocinan, con especial significación en los temas relacionados con la seguridad.

SECCIÓN IV
Análisis de presupuesto

Artículo 9: La etapa de análisis de presupuesto está compuesta por las tareas siguientes:

a) El personal técnico especializado de cada entidad coordinadora en colaboración con los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben, o los que atienden o patrocinan, a partir de la información del levantamiento y los planes de trabajo específicos, elabora los planes de presupuestos e inversiones escalonados en el tiempo, de lo que demande ser cambiado.

b) La entidad coordinadora en la medida que se requiera adquirir nuevos equipamientos y tecnologías por los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben, o los que atienden o patrocinan, para continuar con el normal funcionamiento de sus redes, después de la puesta en vigor de la presente metodología, deben priorizar la adquisición de equipos y tecnologías compatibles con el protocolo IPv6, dar cumplimiento progresivamente según el inventario y el plan de inversiones elaborado y sustituir las existentes que no cumplan con el protocolo IPv6.

SECCIÓN V
Desarrollo de proyectos de pruebas piloto IPv6

Artículo 10: La etapa de desarrollo de proyectos de pruebas piloto IPv6 está compuesta por las tareas siguientes:

a) El responsable del personal técnico especializado de cada entidad coordinadora, una vez cumplimentados los puntos de las etapas precedentes, debe identificar cuáles áreas o proyectos puedan constituirse en proyectos de pruebas pilotos, debido a la disponibilidad de equipamiento y aplicaciones compatibles y que puedan o no necesitar asignaciones experimentales de recursos IPv6, determinan que la red de datos en cuestión está compatibilizada con IPv6 y pueden solicitar al Ministerio de Comunicaciones la autorización para hacer las pruebas pilotos de los proyectos identificados, de acuerdo con lo determinado por la legislación vigente.

b) Las redes que se apruebe que desarrollen pruebas pilotos tienen que funcionar con IPv6 nativo los servidores primarios de segundo nivel y hacer especial énfasis en los temas de seguridad.

CAPÍTULO III
DE LOS INFORMES

SECCIÓN I
De la información a entregar

Artículo 11: Aprobado por el jefe máximo de cada entidad coordinadora, el responsable designado de esta debe informar al Director General de Informática de este ministerio, lo siguiente:

a) A los tres (3) meses a partir de la entrada en vigor de la presente metodología, el responsable y el personal técnico especializado que ha sido designado.

b) A los doce (12) meses a partir de la entrada en vigor de la presente Resolución, un informe parcial consolidado hasta esa fecha, sobre la organización de la preparación del personal en cada entidad y los resultados del levantamiento.
c) A los veinticuatro (24) meses a partir de la entrada en vigor de la presente Resolución, el informe final de los resultados obtenidos en la etapa de levantamiento, la proyección del trabajo y los planes de presupuesto desglosado por cada uno de los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben y o que atienden o patrocinan.

SECCIÓN II
Del formato de la información

Artículo 12: El formato de la información consolidada contenida en los informes a entregar por el responsable de cada entidad coordinadora al Ministerio de Comunicaciones es el siguiente:

a) DE LA ORGANIZACIÓN DE LA PREPARACIÓN DEL PERSONAL:

Información sobre cómo ha organizado la entidad coordinadora, la capacitación en los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben, o los que atienden o patrocinan.

b) DE LOS INFORMES PARCIALES Y FINAL DEL LEVANTAMIENTO DE INFORMACIÓN:

Recursos	Total	De ellos Capacitados para IPv6	%
Personal: 1. Directivos de Tecnologías de la Información. 2. Especialistas y técnicos del área de infraestructura. 3. Especialistas comerciales. 4. Desarrolladores de aplicaciones.			
Recursos	Total	De ellos Compatibles con IPv6	%
Infraestructura: 1. Router (Modelo, IPv6 Ready, S.O., Posibilidad de Actualizar (upgrade)). 2. Switches Gestionables Capa 2 o Capa 3 (Modelo, IPv6 Ready, Sistemas Operativos, Posibilidad de Actualizar (upgrade)). 3. Servidores. 4. Estaciones de trabajo. 5. Otros.			
Servicios (desagregados).			
Aplicaciones (desagregadas).			

c) DE LA PROYECCION DE TRABAJO:

Información sobre el cumplimiento de:

1. La elaboración de los planes de trabajo específicos para realizar los cambios necesarios de forma escalonada en el tiempo, y de los productores de aplicaciones sobre evaluar el rediseño y la puesta en explotación de sus aplicaciones.

2. La modificación a los planes de contingencias.

3. La elaboración de los planes de direccionamiento para la red con direcciones IPv6.

d) DE LOS PLANES DE PRESUPUESTO:

Información sobre el monto total del plan de presupuesto necesario, desglosado por cada uno de los titulares de redes de datos públicas y privadas, que se les subordinan o adscriben, o los que atienden o patrocinan.

SEGUNDO: La Empresa de Telecomunicaciones de Cuba, S. A., en el término de seis (6) meses a partir de la fecha de entrada en vigor de la presente Resolución, presenta a la Dirección General de Comunicaciones de este Ministerio para su aprobación; las tareas y cronogramas de trabajo que permitan operar con IPv6 nativo en adición al funcionamiento con protocolo IPv4, tanto el Punto de Acceso de Red (NAP por sus siglas en inglés); como los enlaces de acceso entre éste y los servidores del proveedor público de acceso a Internet y los servicios fundamentales relacionados al protocolo IPv6, previa conciliación con los órganos de la Defensa, de manera que se puedan acometer los proyectos de pilotos de prueba IPv6 que se autoricen.

TERCERO: El Centro Cubano de Información de Red (CUBANIC) operado por la Empresa de Tecnologías de la Información y Servicios Telemáticos Avanzados (CITMATEL), perteneciente al Ministerio de Ciencia, Tecnología y Medio Ambiente, tiene que lograr que el sistema de nombres de dominio (DNS) del país funcione con IPv6 nativo, a partir de los veinticuatro (24) meses posteriores a la fecha de entrada en vigor de la presente Resolución.

CUARTO: Encargar al Viceministro que atiende la Informatización de este Ministerio:

a) Orientar a las personas jurídicas que son titulares de redes de datos públicas y privadas en el territorio nacional, a través de las entidades coordinadoras, la implementación de la metodología aprobada por la presente Resolución y establecer el mecanismo de control y seguimiento de esta.
b) Evaluar la preparación para la Introducción del Protocolo IPv6 en el país, al finalizar las etapas que se establecen en la Metodología.

QUINTO: Encargar al Director General de Informática del Ministerio de Comunicaciones, la implementación del intercambio vía Web y asesoramiento a las entidades coordinadoras del país, durante el levantamiento de información sobre los equipos, sistemas y aplicaciones compatibles con el protocolo IPv6.

SEXTO: Los órganos de la Defensa adecuan en lo que resulte necesario lo dispuesto en la presente Resolución, en correspondencia con las particularidades de las funciones, misiones y características de las redes de estos.

SÉPTIMO: Encargar a las unidades organizativas del Ministerio de Comunicaciones facultadas para realizar el control y fiscalización, la instrumentación de las medidas que correspondan para exigir el cumplimiento de lo dispuesto en la presente Resolución.

OCTAVO: Derogar la Resolución No. 156 del Ministro de la Informática y las Comunicaciones, de fecha 14 de agosto de 2008.

DÉSE CUENTA a los ministros de las Fuerzas Armadas Revolucionarias, del Interior y de Ciencia, Tecnología y Medio Ambiente y por su conducto a la Directora de la Empresa de Tecnologías de la Información y Servicios Telemáticos Avanzados (CITMATEL).

NOTIFÍQUESE al viceministro que atiende la Informatización y a los directores generales de Informática y de Comunicaciones del Ministerio de Comunicaciones y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A.

COMUNÍQUESE a los directores de Inspección y de Regulaciones y a los directores de las oficinas territoriales de control, todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los días 25 del mes de agosto de 2016.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 71/2015

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en sus numerales Tercero y Decimonoveno del apartado Primero, establece que el Ministerio de Comunicaciones tiene como funciones específicas de proponer, y una vez aprobada, ejecutar y

controlar la política sobre el uso del ciberespacio; así como planificar, implementar, reglamentar, administrar y controlar el sistema de medidas necesarias para su defensa, realizar las coordinaciones internacionales requeridas a ese fin; y de autorizar la asignación de los recursos de numeración de Internet y de uso conjunto a los operadores de servicios público de telecomunicaciones.

POR CUANTO: Resulta conveniente en la gestión de las direcciones de Internet, establecer el Reglamento que aborde los recursos de numeración IP y la elaboración del Plan para su Direccionamiento, con la finalidad de lograr una gestión más ordenada, segura y eficiente de estos recursos en el país y con ello promover el buen uso y control del espacio de las direcciones IP.

POR TANTO: En el ejercicio de las atribuciones delegadas mediante la Resolución No. 1, de fecha 6 de enero de 2015 del Ministro de Comunicaciones;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO PARA EL ORDENAMIENTO DE LOS RECURSOS DE NUMERACIÓN IP

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. El presente Reglamento tiene como objetivo establecer las regulaciones para el ordenamiento de los recursos de numeración de direcciones del protocolo de Internet (dirección IP), aplicable tanto a los proveedores de servicios públicos de acceso a Internet como a los titulares de redes privadas de datos del país los cuales emplean direcciones IP.

Artículo 2. A los efectos del presente Reglamento los términos que se emplean a continuación tienen el significado siguiente:

a) Dirección del protocolo de Internet (IP): Es la cadena o combinación de cifras y símbolos única del protocolo de Internet que identifica los puntos de terminación específicos de una conexión, mediante la asignación a cada dispositivo y terminal que se encuentra en la red, por lo que se utiliza para el encaminamiento de esta.
b) IPv4 e IPv6: Son versiones del protocolo IP, donde la versión 6 (IPv6) fue diseñada para remplazar la versión 4 (IPv4) con una gran cantidad de direcciones entre otros aspectos, debido a que el número máximo de direcciones de red de la versión 4, estaba limitando el crecimiento y uso de Internet.
c) Máscaras de red: Es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras.
d) Recursos de Internet: Recursos que están conformados por las direcciones IP, número de

sistemas autónomos, nombres de dominios y el resultado del proceso de resolución inversa de nombres dominios.

e) Red Privada de Datos: Es aquella infraestructura de red instalada en una misma localidad o en distintas localidades geográficas e interconectadas entre sí por enlaces de telecomunicaciones públicos y propios, administrada y operada por una persona jurídica (Titular) para satisfacer sus necesidades institucionales de transmisión de datos.

f) RFC (Solicitud de Comentarios por sus siglas en inglés): Documento técnico que se elabora y pública por el IETF (Fuerza de Tarea de Ingeniería en Internet) donde se establecen reglas comunes de trabajo en las redes sobre protocolo IP.

Artículo 3. Los Proveedores de Servicios Públicos de Acceso a Internet mantienen actualizada la base de clientes a los que le asignan direcciones IP reales, debiendo entregar copia de la base de datos con la asignación de las direcciones a la Dirección General de Informática del Ministerio de Comunicaciones, el tributo de la información inicial se realiza en el término de cinco (5) días hábiles después de la entrada en vigor la presente Resolución y las actualizaciones a las setenta y dos (72) horas después de realizadas estas.

Artículo 4. Los Proveedores de Servicios Públicos de Acceso a Internet en el proceso de asignación de direcciones IP a sus usuarios, no pueden utilizar direcciones ficticias.

CAPÍTULO II
DE LOS PLANES DE DIRECCIONAMIENTO

Artículo 5. Los titulares de las Redes Privadas de Datos del país elaboran un Plan de Direccionamiento sobre la base de los recursos de numeración IP, en función de su infraestructura de red o su distribución orgánica y delegan las direcciones a las entidades subordinadas teniendo en cuenta el desarrollo de la red y su ulterior actualización.

Artículo 6. El plan refleja una asignación de direcciones IP a cada una de las redes, subredes o nodos de estas para garantizar su conectividad y minimizar vulnerabilidades.

Artículo 7. Los titulares de las redes privadas de datos mantienen constancia actualizada y auditable de los planes de direccionamiento, que se completan con la asignación de direcciones realizada a cada red, subred o nodo en el formato de tablas que se brindan en el Anexo No. 1, a partir de las indicaciones para la elaboración del Plan de Direccionamiento de Recursos de Numeración IP que se encuentran en el Anexo No. 2. Ambos anexos se relacionan formando parte integrante de la presente Resolución.

Artículo 8. El Plan de Direccionamiento elaborado se aprueba por el responsable de la actividad de informática del titular de la red privada de datos, quien también aprueba el procedimiento y los términos para la asignación, así como las condiciones asociadas al uso, las cuales son no discriminatorias y transparentes. En caso de redes privadas que tienen niveles de desagregación, en las subredes o nodos, el Plan lo aprueba el responsable de la actividad de informática de estas y

le envía copia al titular de la red privada de datos.

Artículo 9. El titular de la red privada de datos como parte de la administración de la red, vela por la actualización permanente del Plan de cada red, subred o nodo. Los responsables en cada uno de estos niveles de desagregación mantienen actualizada la documentación con los cambios que se producen, enviando copia de los cambios con respecto a la asignación de direcciones IP reales, al titular de la red privada de datos con la frecuencia que este determine en sus procedimientos y mantener actualizado los cambios de la asignación de direcciones IP ficticias.

Artículo 10. Los titulares de las redes privadas de datos deben entregar copia de la base de datos de los planes de direccionamiento, con la asignación a sus usuarios de las direcciones IP reales, a la Dirección General de Informática del Ministerio de Comunicaciones. El tributo de la información inicial se realiza en el término de cinco (5) días hábiles después de la entrada en vigor de la presente Resolución y las actualizaciones a las setenta y dos (72) horas después de realizadas estas.

CAPÍTULO III
INCUMPLIMIENTOS

Artículo 11. El personal de la Dirección General de Informática y de las oficinas territoriales de control del Ministerio de Comunicaciones, notifica al titular de la entidad encargada de la red privada objeto de control y al responsable de la actividad de informática de la red privada de datos controlada, el incumplimiento en la elaboración y actualización de los Planes de Direccionamiento establecidos por la presente normativa, enviando además copia de la notificación al Director General de Informática de este ministerio.

SEGUNDO: El Director de Regulaciones de este ministerio, queda encargado de proponer la actualización de las reglamentaciones generales para la elaboración y aprobación de los planes de Direccionamiento, teniendo en cuenta las decisiones aplicables que se adopten en las organizaciones y los foros internacionales.

TERCERO: Encargar al Director General de Informática de este ministerio, del almacenamiento y actualización en bases de datos de la información de las direcciones IP reales enviadas por los proveedores de Servicios Públicos de Acceso a Internet y por las redes privadas de datos y de exigir el cumplimiento de lo dispuesto en la presente Resolución, sin perjuicio de que los planes de Direccionamiento puedan ser objeto de control y supervisión por los niveles superiores de la red o los organismos del Estado autorizados, según corresponda.

CUARTO: Se exceptúa a las redes privadas de datos correspondientes a los órganos de la Defensa del envío de sus planes de Direccionamiento a la Dirección General de Informática de este Ministerio.

QUINTO: El presente Reglamento entra en vigor noventa (90) días posteriores a su publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE al Director General de Informática, a los directores de las oficinas territoriales de control y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A., ETECSA, pertenecientes al Ministerio de Comunicaciones

COMUNÍQUESE a los viceministros, a los directores generales de comunicaciones, y de la Oficina de Seguridad de Redes Informáticas y al Director de Regulaciones, todos pertenecientes al Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

DADA en La Habana, a los 31 días del mes de marzo de 2015.

Wilfredo González Vidal
Viceministro en funciones de Ministro

RESOLUCIÓN No. 72/2013

POR CUANTO: El Decreto Ley No. 308 de fecha 23 de febrero de 2013 cambió la denominación Ministerio de la Informática y las Comunicaciones por la de Ministerio de Comunicaciones y establece en su Disposición Especial Única que todas las menciones que en la legislación vigente se hacen respecto al Ministerio de la Informática y las Comunicaciones se consideran referidas al Ministerio de Comunicaciones.

POR CUANTO: El Acuerdo No. 7380, del Consejo de Ministros, de fecha 28 de febrero de 2013, en su numeral Primero, apartado Cuarto establece que el Ministerio de Comunicaciones, es el organismo encargado de ordenar, regular y controlar los servicios de telecomunicaciones, radiocomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos.

POR CUANTO: Nuestro país ha ido creando las condiciones necesarias para adecuar, coordinar y regular las políticas que rigen Internet, de manera tal, que se logre una efectiva organización y funcionamiento de las redes telemáticas que operan los recursos de Internet, teniendo en cuenta que su correcto funcionamiento resulta importante para el desarrollo económico y social del país, por lo que resulta necesario adecuar, coordinar y regular las reglas de trabajo que rigen las redes informáticas y su acceso a Internet, haciéndose por tanto indispensable ordenar el sistema de asignación y registro de los nombres de dominios en las redes privadas de datos de manera tal que se logre una gestión más organizada, segura y eficiente del tráfico nacional e internacional.

POR TANTO: En el ejercicio de la facultad conferida por el numeral Cuarto, apartado Tercero del Acuerdo No. 2817 del Comité Ejecutivo del Consejo de Ministros de fecha 25 de noviembre de 1994;

RESUELVO:

PRIMERO: Aprobar el siguiente:

REGLAMENTO DE LOS NOMBRES DE DOMINIO

CAPÍTULO I
ALCANCE Y DEFINICIONES

Artículo 1. El presente Reglamento tiene como objeto el ordenamiento del sistema de asignación y registro de los nombres de dominio, incluyendo los Planes de nombres de dominio, para el uso en las redes privadas de datos del país.

Artículo 2. Los organismos de la Administración Central del Estado, los órganos locales y superiores del Poder Popular y los órganos del Estado, en cuyos sistemas se encuentran redes privadas de datos, en lo adelante Órganos y Organismos, designan un responsable para la elaboración de las reglas de asignación de los nombres de dominio para el trabajo de las redes privadas de datos de su sistema, las que serán aprobadas por los Jefes de dichos Órganos y Organismos. Dichas reglas serán públicas, transparentes y auditables.

Artículo 3. Los responsables de los Órganos y Organismos quedan encargados de la entrega de las reglas aprobadas y sus posteriores actualizaciones por cualquier motivo, a la Agencia de Control y Supervisión del Ministerio de Comunicaciones, en lo adelante la Agencia.

Artículo 4. Los titulares de redes privadas de datos subordinadas a los Órganos y Organismos, siguiendo las reglas establecidas por los mismos y los titulares de redes privadas de datos no subordinados a estos, son los responsables de la elaboración, aprobación e implementación de los planes de nombres de dominios, teniendo en cuenta las instrucciones generales que se establecen en el presente Reglamento. Estas responsabilidades constituyen el sistema de asignación, además realizarán el registro de los nombres en las entidades autorizadas para ello.

Artículo 5. El Plan debe permitir que el Sistema de Nombres de Dominio (DNS) constituya un servicio de nombres distribuido, jerárquico y escalable con control descentralizado.

Artículo 6. Las definiciones de los términos que se citan a los efectos en el presente Reglamento son:

a) **Asignación de nombres de dominio:** Función de la base de datos del Sistema de Nombres de

Dominio (DNS) que asocia los nombres de dominio con las direcciones IP.

b) **Nombre de dominio:** Identificador compuesto por una serie de nombres delimitados por puntos, usado para la asignación de denominaciones por caracteres alfanuméricos a las direcciones IP para la localización de un equipo o dispositivo (una organización o una persona) o a un conjunto de estos y como mecanismo funcional para localizar un portal o sitio en la red. Su composición como regla es: dominio de nivel superior - subdominio – dispositivo anfitrión (host).

c) **Sistema de Nombres de Dominio (DNS por sus siglas en inglés):** Es el sistema empleado en Internet para poder asignar y usar universalmente nombres unívocos para referirse a equipos, portales o sitios conectados a la red.

d) **Nombre de dominio de nivel superior (TLD por sus siglas en inglés):** Nombre del dominio de máximo nivel superior o raíz, definido a nivel internacional. Se dividen en nombres de dominios genéricos y de código de país.

e) **Nombres de dominios de segundo nivel:** Nombre que se escribe inmediatamente antes del dominio de nivel superior.

f) **Nombre de dominio genérico (gTLD por sus siglas en inglés).** Nombre de dominio de nivel superior de categoría genérica que ofrece una clasificación de acuerdo con el sector de la actividad. Estos pueden ser «.com» (comercio), «.org» (organizaciones), «.tur» (turismo) y otros.

g) **Nombre de dominio geográfico o de código de país (ccTLD por sus siglas en inglés):** Dominio de nivel superior geográfico o de código de país. En el caso de Cuba es «.cu».

h) **Servidores primarios y secundarios de nombre de dominios:** El servidor primario o principal es el que almacena la base de datos distribuida, donde los nombres de dominio son asociados a determinados recursos de Internet. Los servidores secundarios actúan como servidores de reserva para el servidor primario de la misma zona, en caso de que no se pueda tener acceso al servidor principal o esté inactivo.

i) **Servidor con autoridad:** servidor que deberá contener una base de datos con registros que permitan traducir todos los nombres de dominio que estén dentro de su zona a su dirección IP correspondiente.

j) **Zona:** Porción del espacio de nombres de dominio, perteneciente a un dominio y gestionado por un servidor de DNS.

CAPÍTULO II
PLANES PARA NOMBRES DE DOMINIO

Artículo 7. Los titulares de redes privadas de datos, en lo adelante los proveedores, elaboran un plan con los nombres de dominio de menor jerarquía que serán asignados a sus entidades, con una estructura en forma de árbol y en el mismo debe quedar asentado el nombre de la entidad a la que se le asigna cada nombre de dominio.

Artículo 8. El plan de nombres de dominio es aprobado por la máxima dirección de la entidad a la cual pertenece el proveedor.

Artículo 9. En la elaboración del plan, los proveedores tendrán en cuenta que los nombres propuestos deben garantizar que sean exclusivos e inequívocos, de modo que no puedan existir dos nombres de dominio idénticos.

Artículo 10. La organización de los nombres de dominio puede ser según la jerarquía de la estructura organizacional de la institución y también incluir la organización territorial de la misma.

Artículo 11. Los proveedores, en la implementación del plan, asignan a las entidades subordinadas el dominio correspondiente.

Artículo 12. La asignación de nombres de dominio solo otorga derecho de uso del mismo, conforme a lo que se establece en este Reglamento y no representa propiedad, constituye un registro electrónico realizado a nombre de una persona jurídica solicitante, quien ostenta la titularidad.

Artículo 13. Los proveedores administran la zona constituida por los subdominios asignados o delegan, cuando lo decidan, la administración de la zona del subdominio a los administradores de la misma, teniendo en cuenta que cada zona será servida, contando por lo menos con un servidor con autoridad sobre la misma.

Artículo 14. El plan de nombres de dominios y todas las asignaciones que se hagan en su implementación quedarán registrados de forma automatizada en las instalaciones de los proveedores.

Artículo 15. Los proveedores establecen el procedimiento y los plazos para las asignaciones, así como las condiciones asociadas al uso, las cuales serán no discriminatorias y transparentes.

Artículo 16. Los proveedores son responsables de registrar en el CUBANIC los nombres de dominio de mayor jerarquía bajo el ".cu" y a través del propio CUBANIC o del Proveedor Servicios Públicos de Acceso a Internet, hacen el registro en registradores Internacionales de los nombres de dominios bajo la categoría de genéricos de primer nivel, necesarios para el funcionamiento de los servicios de las redes.

Artículo 17. Los nombres de dominio que se generen bajo el nombre de dominio genérico de segundo nivel autorizado en el país, se registran según las reglas de asignación trazadas y las normas establecidas por los propios registradores.

Artículo 18. Los proveedores operan al menos dos servidores de nombres de dominio, uno conocido como primario y otro(s) secundario(s) que pueden localizarse interna o externamente a la organización y tiene en cuenta en su configuración la transferencia de zonas entre ellos.

Artículo 19. Los proveedores quedan obligados a enviar anualmente a la Agencia informes estadísticos de su actividad de asignación y registro, además de informar la contabilización de los tiempos de suspensiones de servicios en sus redes por indisponibilidad del DNS.

Artículo 20. Los proveedores, están obligados a adoptar las medidas necesarias para el cumplimiento de las decisiones que se adopten por el Ministerio de Comunicaciones, en el ámbito de sus competencias sobre nombres de dominio.

CAPÍTULO III
DE LAS MEDIDAS ANTE LOS INCUMPLIMIENTOS

Artículo 21. La Agencia notificará al Jefe de los Órganos y Organismos el incumplimiento de los responsables de la elaboración y entrega de las reglas para la asignación de los nombres de dominio por parte de las redes privadas de datos de su sistema, y se le dará un nuevo plazo de treinta (30) días para su cumplimiento.

Artículo 22. El proveedor que incumpla lo dispuesto en el presente Reglamento está sujeto a la aplicación de las medidas siguientes:

a) Invalidación temporal o definitiva de las licencias de operación de la red privada administrativamente concedidas al titular por la Agencia.
b) Suspensión de los servicios, así como indicar al proveedor de servicios públicos de transmisión de datos y acceso a Internet debidamente reconocido y autorizado por el Ministerio de Comunicaciones, que resuelva los contratos que haya suscrito con el titular del servicio.

Artículo 23. La Agencia, teniendo en cuenta la gravedad de los incumplimientos detectados, así como las consecuencias que implique la aplicación de la medida que corresponda, decide si su aplicación en esta primera instancia es o no de obligatorio cumplimiento a partir de la fecha de su imposición, independientemente del proceso de apelación que se interponga por el titular de la red objeto de la sanción.

Artículo 24. Toda persona jurídica sujeta a la aplicación de las medidas descritas anteriormente, puede apelar en primera instancia ante el Director General de la Agencia, en el término de diez (10) días, contados a partir de la fecha de aplicada la medida, formulando las alegaciones y aportando las pruebas que crea convenientes a su derecho. A su vez el Director General de la Agencia dispone de treinta (30) días para dar respuesta a dicha reclamación.

Artículo 25. Toda persona jurídica que desee impugnar el fallo de la primera instancia de apelación dispone de diez (10) días a partir de la notificación de la misma, para apelar en segunda instancia ante el Ministro de la Informática y las Comunicaciones, a su vez el Ministro dispone de sesenta (60) días para dar respuesta a dicha reclamación. Contra lo dispuesto en esta instancia no cabe ningún otro recurso por vía administrativa.

Artículo 26. El proveedor que ha sido objeto de una sanción que motive su invalidación, suspensión o cancelación de la licencia de operación, puede, resuelta las causas que dieron lugar a la sanción impuesta, volver a presentar a la Agencia su solicitud de inscripción. La Agencia tomando

en cuenta toda la información presentada y comprobada fehacientemente la solución de las deficiencias detectadas decide sobre la nueva inscripción.

SEGUNDO: Los organismos de la Administración Central del Estado, los órganos locales y superiores del Poder Popular y los órganos del Estado tendrán un término de noventa (90) días contados a partir de la entrada en vigor de la presente Resolución para elaborar las reglas para la asignación de los nombres de dominio por parte de las redes privadas de datos de su sistema y hacer entrega de las mismas en la Agencia.

TERCERO: Los proveedores tendrán un término de ciento ochenta (180) días contados a partir de la entrada en vigor de la presente Resolución para tener elaborados y aprobados los planes de nombres de dominio de sus redes privadas.

CUARTO: La Dirección de Regulaciones y Normas, es la encargada de la actualización de las reglamentaciones generales para la elaboración y aprobación de los planes de nombres de dominio, teniendo en cuenta las decisiones aplicables que se adopten en las organizaciones y los foros internacionales.

QUINTO: La Agencia es la encargada de controlar lo establecido en la presente Resolución, sin perjuicio de que los planes para nombres de dominio puedan ser objeto de control, supervisión y auditoría informática por los niveles superiores de la red o los organismos del Estado autorizados, según corresponda.

NOTIFÍQUESE a los Viceministros, al Director de la Dirección de Regulaciones y Normas, a los Directores Generales de la Agencia de Control y Supervisión y de la Oficina de Seguridad de Redes Informática todos pertenecientes al Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

DADA en La Habana, a los 21 días del mes de marzo de 2013.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 132/2011

POR CUANTO: El Acuerdo No. 3736 del Comité Ejecutivo del Consejo de Ministros, de fecha 18 de julio de 2000, en su Apartado Segundo, establece que el Ministerio de la Informática y las Comunicaciones, es el organismo encargado de regular, dirigir, supervisar y controlar la política del Estado y el Gobierno en cuanto a las actividades de tecnologías informáticas, telecomunicaciones,

redes de infocomunicaciones y servicios de valor agregado en infocomunicaciones.

POR CUANTO: El Protocolo IP versión 4 (IPv4) que opera las redes telemáticas que emplean tecnología Internet ha sufrido cambios dados por el desarrollo de esta tecnología y su impacto en la informática y las telecomunicaciones, haciendo que este no sea eficiente por el requerimiento de nuevos servicios y la seguridad de las aplicaciones en línea. Este Protocolo está dando paso a un nuevo Protocolo IP versión 6 (IPv6) que ya es utilizado progresivamente por varios países.

POR CUANTO: La Instrucción No. 5 de fecha 20 de agosto de 2007 de la Dirección de Regulaciones y Normas, estableció el procedimiento para la asignación de direcciones IPv6, para Proyecto Piloto; siendo necesario por el tiempo transcurrido, la experiencia adquirida de su aplicación y la necesidad de agilizar la introducción del IPv6 en todas las instituciones del país, se emita una nueva norma jurídica de mayor rango, que regule mediante un procedimiento la autorización de Proyectos Pilotos con Direcciones IP versión 6, lo que coadyuvará a que las redes privadas datos de organizaciones y entidades nacionales que de manera experimental y con fines investigativos, así lo soliciten. Esta nueva disposición una que vez emitida va a contribuir a ejecutar el contenido de la Resolución Ministerial No. 156 de fecha 14 de agosto del 2008, que aprobó la Metodología para la Introducción del Protocolo IPv6 en las Redes Telemáticas, Sistemas Informáticos y Aplicaciones de Software en el país.

POR TANTO: En el ejercicio de la facultad conferida por el numeral Cuarto, Apartado Tercero del Acuerdo No. 2817 del Comité Ejecutivo del Consejo de Ministros, de fecha 25 de noviembre de 1994;

RESUELVO:

PRIMERO: Aprobar el siguiente:

PROCEDIMIENTO PARA LA AUTORIZACIÓN DE PROYECTOS PILOTOS CON DIRECCIONES IP VERSIÓN 6 A LOS TITULARES DE REDES PRIVADAS DE DATOS

Artículo 1: Corresponde al titular de las redes privadas de datos de organismos, organizaciones y entidades nacionales, en lo adelante solicitante, realizar la petición de aprobación de proyectos pilotos con direcciones IP versión 6 a la Dirección de Regulaciones y Normas.

Artículo 2: Las solicitudes se realizan en formato de papel impreso y en digital, de acuerdo a los formularios que se establecen y que aparecen en los anexos .1 y 2, los cuales deben presentarse junto con los documentos siguientes:

1. Carta aval del responsable del organismo, de organizaciones y entidades nacionales que autoriza la Propuesta del Proyecto Piloto.
2. Constancia de registro de la red privada de datos emitido por la Agencia de Control y Supervisión, en lo adelante la Agencia.

Artículo 3: Corresponde al solicitante cumplir además los deberes siguientes:

1. Gestionar a solicitud propia de no poseer direcciones IPv6 ante el Proveedor de Servicio Público de Acceso a Internet (ISP), las direcciones IPv6 para el desarrollo del Proyecto Piloto, previamente aprobado por la Dirección de Regulaciones y Normas.
2. Evaluar semestralmente los consumos de tráfico IPv6 cursados por su red privada y efectuar su análisis de conjunto con el Proveedor de Servicio Público de Acceso a Internet.
3. Informar al Viceministro que atiende la Informática, en lo adelante Viceministro, con periodicidad semestral la marcha del proyecto piloto aprobado, así como cualquier caso de discrepancia relacionada con dichas solicitudes de servicios.
4. Elaborar un informe de conclusiones, al finalizar el proyecto piloto y enviar una copia de este al Viceministro.
5. Utilizar las direcciones IPv6 del proyecto piloto aprobado solo en servicios dentro su red privada.

Artículo 4: Corresponde a la Dirección de Regulaciones y Normas, los deberes siguientes:

1. Notificar por escrito al solicitante la aprobación o denegación del Proyecto Piloto con direcciones IP versión 6 solicitado, en un plazo no mayor de quince (15) días hábiles, una vez recibida la solicitud por la Dirección de Regulaciones y Normas, enviando una copia de la notificación, en caso de la aprobación, a los Proveedores de Servicio Público de Acceso a Internet, a la Oficina para la Informatización y al Viceministro.
2. Convocar, de ser necesario, a un grupo de expertos para la evaluación técnica y viabilidad de las propuestas de Proyectos Pilotos.
3. Solicitar semestralmente al Viceministro, información del estado de ejecución de los Proyectos Pilotos, así como el informe de conclusiones al finalizar el mismo.
4. Suspender la ejecución de un Proyecto Piloto, a partir de la solicitud de la Oficina para la Informatización, en el caso de hacerse un uso de las direcciones IPv6 diferente del aprobado.

Artículo 5: Corresponde a los Proveedores del Servicio Público de Acceso a Internet cumplir con los deberes siguientes:

1. Recibir las solicitudes de direcciones IPv6 de las redes privadas de datos que no la posean y asignarlas según lo aprobado por la Dirección de Regulaciones y Normas.
2. Informar a la Agencia las direcciones IPv6 asignadas.
3. Garantizar el servicio del Sistema de Nombres de Dominio (DNS), así como la ruteabilidad de las direcciones IPv6, tanto las asignadas al solicitante, como las que este haya adquirido directamente de la Organización para el Registro de Direcciones de Internet de América Latina y el Caribe (LACNIC) y que se corresponden con el Proyecto Piloto aprobado por la Dirección de Regulaciones y Normas.
4. Las asignaciones de direcciones IPv6 que se realicen, no serán nunca mayores que un /48 (“barra 48”) (1.2 * 10 24) de direcciones IP.
5. Firmar con cada uno de los solicitantes de direcciones IPv6 el contrato correspondiente o su

actualización, dejando claramente establecido en el mismo el tipo de servicio, los parámetros de calidad que son garantizados y demás cláusulas que correspondan.

6. Evaluar semestralmente los consumos de tráfico de los servicios contratados al Proveedor de Servicio Público de Acceso a Internet y efectuar análisis de conjunto con el solicitante acerca del comportamiento de los mismos.
7. Informar al Viceministro, cualquier caso de discrepancia relacionada con dichas solicitudes de servicios.

Artículo 6: Corresponde al Viceministro.

1. Requerir semestralmente de las entidades responsables del proyecto piloto con direcciones IP versión 6 autorizado por la Dirección de Regulaciones y Normas, información del estado de ejecución de los mismos; así como el informe de conclusiones al finalizar cada Proyecto Piloto, enviando copia de estos a la Dirección de Regulaciones y Normas. Coordinar la publicación Web de los resultados que resulten de interés para las redes privadas del país.
2. Solicitar a la Dirección de Regulaciones y Normas la suspensión de la ejecución de un Proyecto Piloto, en el caso de hacerse un uso de las direcciones IPv6 diferente del aprobado.
3. Conocer acerca de las discrepancias recibidas del Proveedor de Servicio Público de Acceso a Internet y las relacionadas con las solicitudes de servicios para la ejecución del Proyecto Piloto con direcciones IPv6.
4. Dar a conocer en un término de siete (7) días hábiles sus conclusiones al respecto al Proveedor de Servicio Público de Acceso a Internet y a la entidad responsable de la ejecución del proyecto.

SEGUNDO: Derogar la Instrucción No. 5 de fecha 20 de agosto de 2007, de la Dirección de Regulaciones y Normas.

NOTIFÍQUESE al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A., a la Directora de la Empresa de Tecnologías de la Información y Servicios Telemáticos, CITMATEL, perteneciente al Ministerio de Ciencias, Tecnología y Medio Ambiente.

COMUNÍQUESE a los Viceministros, a los Directores de Regulaciones y Normas, Oficina para la Informatización y al Director General de la Agencia de Control y Supervisión, pertenecientes al Ministerio de la Informática y las Comunicaciones, a los Titulares de las redes privadas de datos y a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

DADA en La Habana, a los 19 días del mes de agosto de 2011.

Medardo Díaz Toledo
Ministro

ANEXO 1
RESOLUCIÓN No. 132/2011

PLANILLA PARA LA NOMINALIZACIÓN DE PROYECTO PILOTO

Nombre del proyecto: Entidad que solicita: Organismo: Objetivos:
Responsables de proyecto: Breve descripción: Resultados esperados: Área de aplicación:
Fecha de inicio: Fecha de terminación:
Nota: Enviar copia en formato digital.

ANEXO 2
RESOLUCIÓN No. 132/2011

PLANILLA SOBRE LAS DIRECCIONES IPv6

I.- Información sobre la organización, institución o entidad que está solicitando realizar proyecto piloto con direcciones IPv6.

1. Nombre de la organización, institución o entidad:
2. Dirección postal
3. Datos de contacto. (Nombres, Apellidos, e-mail, dirección postal del lugar de localización)
   Contacto técnico: (correo-e)
   Contacto administrativo: (correo-e)

II.- Información de la red IPv6 propuesta para el desarrollo del proyecto piloto. Especificar:

a) Direccionamiento IPv6:
b) Plan de utilización.
c) Plan de asignación.
d) Plan de despliegue de la organización, institución o entidad.
   1. Presentar estructurado el proyecto en distintas fases de pruebas. En cada una plantear lo que abarcan las mismas, especificando que método de transición seria utilizado, topología de la red, servicios propuestos, el alcance de los mismos, puntos de supervisión y cronograma de implementación.
   2. Características principales de la tecnología a emplear y suministrador de la misma.
   3. Para cada fase de pruebas especificar los lugares geográficos donde se encuentran los distintos nodos de la red privada a interconectar, indicando los segmentos que atraviesan por la red pública, y en caso de ser necesario esto, determinar la velocidad de transmisión que sería requerida para dicho segmento.
   4. Aspectos de seguridad de redes involucrados.
   5. Forma de gestión a proponer.

III. Fecha:

RESOLUCIÓN No. 178/2008

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000, cambió la denominación del Ministerio de Comunicaciones por la de Ministerio de la Informática y las Comunicaciones, para que desarrollara las tareas y funciones que realizaba el Ministerio de Comunicaciones, así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sidero- Mecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 30 de agosto del 2006, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: De conformidad con el Acuerdo No. 2817 de fecha 25 de noviembre de 1994 del Comité Ejecutivo del Consejo de Ministros, corresponde a los Jefes de los Organismos de la Administración Central del Estado; dictar, en el límite de sus facultades y competencia, reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del Organismo; y en su caso, para los demás organismos, órganos locales del poder popular, las entidades estatales, el sector cooperativo, mixto, privado y la población.

POR CUANTO: El Acuerdo No. 3736 de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo del Consejo de Ministros, establece que el Ministerio de la Informática y las Comunicaciones, en lo adelante el MIC, es el organismo encargado de ordenar, regular y controlar los servicios informáticos y de telecomunicaciones, nacionales e internacionales y otros servicios afines en los límites del territorio nacional; así como, de conjunto con las organizaciones correspondientes, el acceso a las redes de infocomunicaciones con alcance global.

POR CUANTO: Mediante la Resolución Ministerial No. 195 de fecha 17 de diciembre del 2007, se emitió el Reglamento de Redes Propias de Datos, por lo que resulta necesario implementar un conjunto de reglas que ordenen el proceso de categorización de las Redes Propias de Datos que existen en el país, a fin de que el personal que labora en las mismas, esté en correspondencia con la categoría de dichas redes, atemperándose a las exigencias del desarrollo alcanzado en las nuevas tecnologías, los servicios, las condiciones especiales de trabajo derivadas de la complejidad de la red y el uso racional de los recursos.

POR TANTO: En el ejercicio de las facultades que me están conferidas,

RESUELVO:

PRIMERO: Aprobar el Reglamento de Categorización de las Redes Propias de Datos que aparece en el anexo a la presente Resolución, formando parte integrante de la misma.

SEGUNDO: Las entidades que posean Redes Propias de Datos, deben adoptar en los casos en que se disponga para la categorización de dichas redes, el proceso de evaluación que se aprueba por la presente Resolución. Como proceso complementario deben solicitar a su nivel jerárquico superior,

Organismo, Organización u Órgano del Poder Popular al que pertenezcan, la certificación de la categorización resultante a partir de la evaluación realizada.

TERCERO: La Dirección de Regulaciones y Normas de este Ministerio, en un término de ciento ochenta días posteriores a la fecha de entrada en vigor del Reglamento que por la presente se establece, deberá conformar el procedimiento que cree y ordene el funcionamiento de la Comisión Interministerial para el otorgamiento de la condición de especial, asimismo, queda encargada de dictar las disposiciones complementarias que resulten necesarias para el cumplimiento de lo que por la presente se dispone.

CUARTO: Encargar a la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, la instrumentación de las medidas que considere necesarias para el mejor cumplimiento de lo establecido en la presente Resolución.

QUINTO: Se exceptúan del cumplimiento de la presente, los Ministerios de las Fuerzas Armadas Revolucionarias y del Interior, los que establecerán sus normativas y controles para sus respectivos sistemas.

NOTIFÍQUESE a los Viceministros, a la Dirección de Regulaciones y Normas, Economía, Recursos Humanos, a la Oficina de Informatización, a la Oficina de Seguridad para las Redes

Informáticas, y a la Agencia de Control y Supervisión, todas pertenecientes al Ministerio de la Informática y las Comunicaciones.

COMUNÍQUESE a los Jefes de Organismos de la Administración Central del Estado y a cuantas personas naturales y jurídicas deban conocer de lo dispuesto.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los días 7 del mes de octubre del 2008.

Ramiro Valdés Menéndez
Ministro

ANEXO - RESOLUCIÓN No. 178/2008
REGLAMENTO DE CATEGORIZACIÓN DE REDES PROPIAS DE DATOS

CAPÍTULO I
OBJETO Y ALCANCE

Artículo 1: En el presente Reglamento se establecen las disposiciones específicas para organizar los procesos de evaluación y certificación para la Categorización de las Redes Propias de Datos que existen en el país, en lo adelante la Red.

Artículo 2: Los términos que se emplean en este Reglamento, tienen el significado siguiente:

a) **Protocolo de comunicación:** Conjunto de reglas y formatos, semánticos y sintácticos, que determina el comportamiento de comunicación de determinadas actividades en la realización de las funciones que correspondan, entre otros, Protocolos X-25, ATM o IP.
b) **Red Propia de Datos:** Infraestructura de red instalada en una misma localidad o en distintas localidades geográficas e interconectadas entre sí, por enlaces de telecomunicaciones públicos y propios, administrada y operada por una persona jurídica, o titular, para satisfacer sus necesidades institucionales de Transmisión de Datos.
c) **Terminal:** Utilizado como una generalización de “Equipo terminal de usuario”, es el equipo asociado al usuario final que se encuentra conectado, o con capacidad de conectarse, funcionalmente a redes de telecomunicaciones para acceder a uno o más de los servicios que se prestan a través de éstas.
d) **Usuario:** Es aquella persona natural o jurídica que, en forma eventual o permanente, utiliza algún servicio público o privado de telecomunicaciones.
e) **Entidad:** De los Organismos de la Administración Central del Estado, los Órganos Estatales y sus unidades o dependencias administrativas y demás unidades presupuestadas, las empresas estatales y las uniones de empresas estatales; las organizaciones políticas, sociales y de masas, sus empresas y unidades dependientes, las Cooperativas de producción y sus dependencias; empresas nacionales y cualquier otra con capacidad y personalidad jurídica propia; así como cualquier otra estructura organizativa de conformidad con la legislación vigente en el país.

CAPITULO II
DE LA CATEGORIZACION DE LAS REDES PROPIAS DE DATOS

Artículo 3: La Categorización de la Red de cada entidad es el resultado del proceso de evaluación de la misma, del cual se puede obtener uno de los niveles que se relacionan a continuación:

1. Red de elevada complejidad: categoría A.
2. Red de mediana complejidad: categoría B.
3. Red de baja complejidad: categoría C.

Artículo 4: Puede existir además en el proceso de categorización, la posibilidad de solicitar la condición de Red Especial, de acuerdo a lo establecido en el Capítulo IV del presente Reglamento.

Artículo 5: La Categorización de la Red se realiza a partir de la evaluación de un conjunto de indicadores, como son:

a) Alcance geográfico.
b) Agrupación de los usuarios en la red.
c) Tipo de terminales conectadas.
d) Cantidad de terminales conectadas
e) Protocolos de comunicación y sistemas de operación.
f) Empleo del operador (administrador, supervisor) en el servicio de red.
g) Gestión de infraestructura propia.
h) Tipo de acceso por los usuarios de la red.
i) Servicios implementados en la red.
j) Requisitos de seguridad de las tecnologías de la información en la red.

Artículo 6: Para la categorización de la Red se selecciona en cada indicador, conforme al anexo 1, el elemento que mejor caracteriza la red de la entidad, tomando la puntuación correspondiente a la columna peso que corresponde al elemento.
El peso de los elementos de cada indicador, refleja la cantidad de esfuerzo requerido a los trabajadores a cargo de la Red.
El resultado de la evaluación de los indicadores de la Red con el propósito de su categorización, se reflejará utilizando el modelo 2.1 del anexo 2 y la metodología para su confección expuesta en el anexo 3.

Artículo 7: La evaluación para la categorización de la Red, la aprueba el jefe máximo de cada entidad y la ejecuta el personal especializado que el mismo designe, lo cual se reflejará en el modelo 2.1 del anexo 2.

CAPITULO III
DEL EXPEDIENTE Y LA CERTIFICACIÓN DE LA CATEGORIZACIÓN DE REDES PROPIAS DE DATOS

Artículo 8: La evaluación realizada por cada entidad es certificada por el nivel jerárquico superior de dirección de la misma. El jefe máximo del nivel superior de la red de la entidad que ejecutó la evaluación, puede delegar esta acción, en cuyo caso se creará el correspondiente registro incorporando los datos del designado, conforme se establece en el modelo 2.2 del anexo 2.

Artículo 9: Como resultado del proceso de evaluación, se conforma un expediente de categorización cuyo contenido será el siguiente:

a) La información oficial sobre los registros que posee la entidad sobre su red, como es la Licencia emitida por la Agencia de Control y Supervisión del MIC.
b) El modelo 2.1 del anexo 2, Evaluación de los Indicadores, Definición y Certificación de la Categoría de la Red, con el resultado del proceso de evaluación para la categorización realizada y su certificación, debidamente firmado y acuñado.
c) El modelo 2.2 del anexo 2, Registro de la Autoridad Facultada para la Certificación de la Categoría de la Red, debidamente firmado y acuñado, en el caso de que exista delegación de esta actividad.
d) La Tabla correspondiente al anexo 1.

Artículo 10: El expediente de categorización debe permanecer en la entidad, copia del modelo 2.1 con el resultado de la categorización realizada y su certificación se enviará a la Agencia de Control y Supervisión del MIC, a los efectos del control estadístico por categoría de las de redes certificadas.

Artículo 11: Los datos declarados y el expediente de categorización pueden ser objeto de comprobación por las autoridades estatales que corresponda. De detectarse violación de lo establecido en el presente Reglamento, la categoría certificada quedara invalidada, procediendo la autoridad a notificar a la entidad violadora para que emprenda un nuevo proceso de evaluación y la certificación de sus resultados.

Artículo 12: Se exceptúan de realizar el proceso de certificación, las oficinas centrales de los Organismos de la Administración Central del Estado y de las Organizaciones Políticas y de Masas y los Órganos Provinciales del Poder Popular. En estos casos el modelo 2.2 no aparecerá en su expediente de categorización.

CAPITULO IV
DE LA VALORACION COMPLEMENTARIA DE LA CONDICION DE ESPECIAL

Artículo 13: En el proceso de categorización es posible la asignación complementaria de la condición de Red Especial, con el objetivo de otorgar un mayor valor a la categoría que se haya obtenido como resultado del cálculo realizado durante el proceso de evaluación.

Artículo 14: La Red puede ser declarada especial por poseer condiciones estratégicas para la defensa nacional o por tener un gran impacto sobre los servicios a la población o la economía del país.

Artículo 15: El otorgamiento de la condición de especial a una red se establece por una Comisión Interministerial, que se convoca para analizar la solicitud recibida en este Ministerio, de la máxima representación del Organismo, Organización u Órgano del Poder Popular al que pertenezca dicha Red, y será otorgada por decisión propia del MIC o a propuesta de los órganos de la defensa.

Anexo 1
INDICADORES Y PESOS PARA LA CATEGORIZACIÓN DE REDES

INDICADORES	PESO
ALCANCE GEOGRAFICO	
Red Local	1
Red de Campo	7
Municipal	8
Provincial	9
Regional	10
Nacional	15
Internacional	17
AGRUPACION DE LOS USUARIOS EN LA RED	
Sector de la Economía o la Sociedad	10
Grupo Unión o Corp., Empresarial o Institucional	5
Unidad administrativa empresarial de base o establecimiento, Unidad presupuestada, Empresa o Unidad básica	1
TIPO DE TERMINALES CONECTADAS	
Unidades de tarjetas magnéticas, cajas registradoras	1
Cajeros automáticos	3
Equipamiento computacional de escritorio	4
Servidores (medios de computación corrientes en funciones de servidores)	5
Servidores Profesionales (medios de computación especialmente construidos para servidor)	8
CANTIDAD DE TERMINALES CONECTADAS	
Desde 1 hasta 249	1
Desde 250 hasta 499	5
Más de 500	9
PROTOCOLOS DE COMUNICACION Y SISTEMAS DE OPERACION	
X-25 y SO basado en asistentes	1
Frame Relay y/o SO basado en comandos y ficheros de configuración	3
ATM y/o SO basado en comandos y ficheros de configuración	4
IP y/o SO basado en comandos y ficheros de configuración	5
Multiservicio o multiprotocolo y SO basados en asistentes y en comandos	8
EMPLEO DEL OPERADOR (ADMINISTRADOR, SUPERVISOR) EN EL SERVICIO DE RED	
Con operadores tiempo completo	12
Con operadores tiempo parcial y alarmas	11
Operadores días laborables y alarmas	6
Operadores días laborables	1

GESTION DE INFRAESTRUCTURA PROPIA	
Más de 12 nodos (subredes)	9
Desde 5 nodos hasta 11	5
Desde 1 hasta 4 nodos	1

TIPOS DE ACCESO POR LOS USUARIOS DE LA RED	
Conmutado con RAS o PAP y Dedicado	10
Dedicado	5
Conmutado	1

SERVICIOS IMPLEMENTADOS EN LA RED	
Correo nacional, navegación nacional y FTP	1
Correo nacional e internacional, navegación nacional e internacional y FTP	4
Correo y navegación nacional e internacional, FTP y mensajería instantánea	5
Correo y navegación nacional e internacional, FTP, mensajería instantánea y otros servicios (aplicaciones, VoIP, VoD, transacciones bancarias)	10

REQUISITOS DE SEGURIDAD DE LAS TECNOLOGIAS DE LA INFORMACION EN LA RED	
Requisito de confidencialidad, integridad y disponibilidad alto	10
Requisito de confidencialidad, integridad y disponibilidad medio	6
Requisito de confidencialidad, integridad y disponibilidad bajo	1

Anexo 2
Resolución No. 178/2008

2.1 MODELO EVALUACIÓN DE LOS INDICADORES, DEFINICIÓN Y CERTIFICACIÓN DE LA CATEGORIA DE LA RED

Nombre de la entidad: **INDICADORES:**	**Código REEUP de la entidad: Puntuación Obtenida**
A). ALCANCE GEOGRÁFICO	
B) AGRUPACION DE LOS USUARIOS EN LA RED	
C) TIPO DE TERMINALES CONECTADAS	
D) CANTIDAD DE TERMINALES CONECTADAS	
E) PROTOCOLOS DE COMUNICACIONES	
F) EMPLEO DEL OPERADOR EN EL SERVICIO DE RED	
G) GESTIÓN DE INFRAESTRUCTURA PROPIA	
H) TIPOS DE ACCESO POR LOS USUARIOS A LA RED	
I) SERVICIOS IMPLEMENTADOS EN LA RED	
J) REQUISITOS DE SEGURIDAD	
TOTAL	

Categoría de la Red de Datos:

Funcionarios que evaluaron:			
Nombres y Apellidos:	Cargo:	Firma:	Fecha:

Autoridad que aprobó:			
Nombres y Apellidos:	Cargo:	Firma:	Fecha:

Autoridad que certificó:			
Nombres y Apellidos:	Cargo:	Firma:	Fecha:

2.2 MODELO AUTORIDAD FACULTADA PARA LA CERTIFICACIÓN DE LA CATEGORIZACIÓN

Nombre de la entidad:	Código REEUP de la entidad:		
Nombre de la Organización que CERTIFICA:	Código REEUP:		
Autoridades a las que se les delega la certificación:			
Nombres y Apellidos:	Cargo:		Fecha:
Autoridad máxima del nivel jerárquico superior:			
Nombres y Apellidos:	Cargo:	Firma:	Fecha:

Anexo 3
Resolución No. 178/2008

METODOLOGÍA DE CONFECCIÓN DEL MODELO B1 DE EVALUACIÓN DE LOS INDICADORES, DEFINICIÓN Y CERTIFICACIÓN DE LA CATEGORÍA DE LA RED

Se procederá a llenar el modelo de la forma siguiente:

PRIMERA ETAPA: POR PARTE DE LA ENTIDAD.

Nombre de la entidad:

Se especifica la denominación completa de la entidad y las siglas o acrónimo que la identifica.

Código REEUP de la entidad:

Se indica el código que posee la entidad del correspondiente al clasificador de actividades económicas.

Puntuación Obtenida (columna 2):

Para cada indicador de la columna 1 (A, B, C) se decide, utilizando la Tabla 2.1 del anexo 1, aquel y solo aquel atributo que mejor caracteriza a la red evaluada, tomando el puntaje que corresponda según el peso asignado a dicho atributo.

En el caso de que la red de la entidad esté caracterizada por más de un atributo en alguno de los indicadores, se tomará la puntuación relativa al atributo de mayor peso.

La fila total reflejará entonces el valor resultante de la métrica:

V=∑ PO i

o sea, la suma de la puntuación obtenida (PO) por cada indicador, a saber: V= PO (A) + PO (B) +PO (C) + PO (D) + PO (E) + PO (F) + PO (G) + PO (H) + PO (I) + PO (J)

Categoría de la Red de Datos:
Se selecciona la categoría a partir de valor resultante obtenido:

VALOR RESULTANTE (V)	CATEGORÍA
71 a 100	A
36 a 70	B
35 o menos	C

Funcionarios que evaluaron:
Se indican los nombres, cargos y fecha de realización de la evaluación, reflejando sus firmas.

Autoridad que aprobó:
Se indica el nombre, cargo y fecha de la aprobación por la máxima autoridad de la entidad, reflejando su firma y el cuño correspondiente.

SEGUNDA ETAPA: POR PARTE DEL NIVEL JERÁRQUICO SUPERIOR A LA ENTIDAD

Autoridad que certificó:

Se indica el nombre, cargo y fecha de la certificación por la máxima autoridad del nivel jerárquico superior de la entidad, reflejando su firma y cuño.
Si la máxima autoridad del nivel jerárquico superior de la entidad hubiere delegado esta acción, se procederá a firmar por la misma el modelo 2.2 Autoridad Facultada para la Certificación de la Categorización Propuesta.

RESOLUCIÓN No. 138/2008

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000 cambió la denominación del Ministerio de Comunicaciones por el de Ministerio de la Informática y las Comunicaciones, para que desarrollara las tareas y funciones que realizaba el Ministerio de Comunicaciones, así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sideromecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 30 de agosto del 2006, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: El Acuerdo No. 2817 de fecha 28 de noviembre de 1994, del Comité Ejecutivo del Consejo de Ministros, faculta a los Jefes de los Organismos de la Administración Central del Estado; a dictar en el límite de sus facultades y competencia, reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del organismo, sus dependencias y en su caso, para los demás

organismos, los órganos locales del poder popular, las entidades estatales, el sector cooperativo, mixto, privado y la población.

POR CUANTO: El Acuerdo No. 3736, de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo del Consejo de Ministros, establece que el Ministerio de la Informática y las Comunicaciones, en lo adelante MIC, es el organismo encargado de ordenar, regular y controlar los servicios informáticos, de telecomunicaciones y postales, nacionales e internacionales y otros servicios afines en los límites del territorio nacional, así como, de conjunto con las organizaciones correspondientes, el acceso a las redes de infocomunicaciones con alcance global. Establece además que es el organismo encargado de la gestión de los recursos comunes y escasos en materia de dichos servicios, así como de proponer y controlar las prioridades para la implementación de estos.

POR CUANTO: Los Organismos Internacionales que hoy operan las Direcciones IP, Números de Sistemas Autónomos (ASN), Sistemas de Nombre de Dominios y Resolución Inversa de Dominios, en lo adelante Recursos de Internet, han ido ganando en organización, atendiendo los cambios de innovaciones tecnológicas que se producen a escala mundial, lo que les ha permitido una mayor regulación y control de las políticas que hoy la rigen.

POR CUANTO: Nuestro país debe crear las condiciones necesarias para adecuar, coordinar y regular las políticas que rige Internet, de manera tal que se logre una efectiva organización y funcionamiento de las Redes Telemáticas en el país que operan los Recursos de Internet, acorde a las necesidades de lograr una gestión más ordenada, segura y eficiente del tráfico de Internet nacional e internacional, teniendo en cuenta que su correcto funcionamiento es importante para el desarrollo económico y social del país.

POR CUANTO: Resulta necesario ordenar y controlar las solicitudes de las Direcciones IP, Números de Sistemas Autónomos (ASN), Sistemas de Nombre de Dominios y Resolución Inversa de Dominios, identificados como Recursos de Internet, que se realizan ante el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC) por parte de las organizaciones o entidades nacionales o extranjeras, radicadas en territorio nacional.

POR TANTO: En el ejercicio de las facultades que me están conferidas,

RESUELVO:

PRIMERO: Los Proveedores de Servicios Públicos y Propios de Internet, en lo adelante Solicitantes, debidamente reconocidos ante la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, MIC, son los encargados de realizar la solicitud de Recursos de Internet a LACNIC, previa aprobación de ésta por la Dirección de Regulaciones y Normas de este Ministerio.

SEGUNDO: Los Solicitantes deben realizar las siguientes acciones ante la Dirección de Regulaciones y Normas del MIC:

1. Presentar carta de solicitud, firmada por el Titular de la Red, expresando la necesidad de recibir asignación de Recursos de Internet.
2. Presentar certifico actualizado de su Registro de Red Propia otorgado por la Agencia de Control y Supervisión.
3. Presentar en formato digital copia de las planillas de solicitud requeridas por LACNIC debidamente llenada.

TERCERO: Corresponde a la Dirección de Regulaciones y Normas las siguientes funciones:

1. Notificar por escrito al Solicitante, la denegación o aceptación de la solicitud de Recursos de Internet con copia, de ser aceptada, a la Agencia de Control y Supervisión del MIC y al Proveedor Público de Servicio de Internet que corresponda, en un plazo no mayor de siete (7) días hábiles.
2. Archivar y custodiar debidamente los expedientes que genere las solicitudes de Recursos de Internet recibidas.

CUARTO: Corresponde a los Proveedores Públicos de Servicio de Internet anunciar sólo los Recursos de Internet autorizados por la Dirección de Regulaciones y Normas del MIC.

QUINTO: Corresponde a los Solicitantes cumplir las siguientes funciones:
1. Gestionar, a solicitud propia ante LACNIC, los Recursos de Internet previamente aprobados por la Dirección de Regulaciones y Normas.
2. Registrar en la Agencia de Control y Supervisión del MIC el Recurso adjudicado por LACNIC.

SEXTO: Los Recursos de Internet que actualmente están asignados por LACNIC, o fueron asignados por InterNIC, antigua empresa dedicada al registro de direcciones IP, actualmente extinta, y se encuentran en uso, se ratifican por la Dirección de Regulaciones y Normas previo registro en la Agencia de Control y Supervisión del MIC y una vez recibida dicha notificación.

SÉPTIMO: Con la entrada en vigor de la presente Resolución se consideran nulos aquellos Recursos asignados, o que en un futuro lo sean, por otros Registradores Internacionales de Recursos de Internet diferentes a LACNIC.

OCTAVO: La Dirección de Regulaciones y Normas del Ministerio de la Informática y las Comunicaciones es la encargada de proponer al que resuelve, las disposiciones complementarias a la presente resolución.

NOVENO: Encargar a la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, establecer las medidas de control y supervisión pertinentes para garantizar el cumplimiento de lo dispuesto en esta.

COMUNÍQUESE a los Viceministros, a la Dirección de Regulaciones y Normas, a las Entidades Proveedoras de Servicios de Internet, Públicos y Propios, a la Agencia de Control y Supervisión, a los Titulares de Redes Públicas y Propias de Datos y a cuantas personas naturales o jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en la ciudad de La Habana, a los días 6 del mes de junio del 2008.

Ramiro Valdés Menéndez
Ministro

RESOLUCIÓN No. 194/2007

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000, cambió la denominación del Ministerio de Comunicaciones por la de Ministerio de la Informática y las Comunicaciones, que desarrollará las tareas y funciones que hasta el presente realizaba el Ministerio de Comunicaciones, así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sidero-Mecánica y la Electrónica.

POR CUANTO: Mediante la Resolución No. 182 de fecha 4 de diciembre del 2007 el Ministro de la Informática y las Comunicaciones, delegó temporalmente en quien suscribe, todas las facultades y atribuciones inherentes a su cargo.

POR CUANTO: El Acuerdo No. 2817 de fecha 25 de noviembre de 1994, del Comité Ejecutivo del Consejo de Ministros, faculta a los Jefes de los Organismos de la Administración Central del Estado; a dictar en el límite de sus facultades y competencia, reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del organismo; y, en su caso, para los demás Organismos, Los Órganos Locales del Poder Popular, las Entidades Estatales, el Sector Cooperativo, Mixto, Privado y la Población.

POR CUANTO: El Acuerdo No. 3736 de fecha 18 de julio del 2000, del Comité Ejecutivo del Consejo Ministros, facultó al Ministerio de la Informática y las Comunicaciones a establecer, regular y controlar la política y las estrategias para el desarrollo, la evolución, la producción, la comercialización y la utilización de los servicios y tecnologías de la informática y las comunicaciones, el desarrollo y evolución de la industria electrónica y la automatización, el desarrollo de la infraestructura de las redes de infocomunicaciones, de los servicios de valor agregado, de los servicios postales, y de conjunto con los

organismos correspondientes, el acceso a las redes de infocomunicaciones con alcance global.

POR CUANTO: La Concesión Administrativa del Servicio Público de Telecomunicaciones, otorgada en el Decreto No. 275 de fecha 16 de diciembre del 2003, emitido por el Comité Ejecutivo del Consejo de Ministros, en el Capítulo II sobre el Alcance de la Concesión, especifica los servicios que prestará la Empresa de Telecomunicaciones de Cuba S.A., ETECSA, en exclusividad por el período enmarcado en dicha concesión.

POR CUANTO: Los Sistemas de Comunicaciones por Líneas Eléctricas, conocidos como PLC, se basan en una tecnología de transmisión de datos de banda ancha que utiliza como infraestructura la red eléctrica, ello posibilita mediante estos sistemas cualquier servicio basa- do en Protocolos de Internet.

POR CUANTO: Los Sistemas de Comunicaciones de Banda Ancha por Líneas Eléctricas, constituyen un medio económico para hacer llegar las comunicaciones de Banda Ancha a to- dos los lugares donde exista distribución del servicio eléctrico, por lo que resulta conveniente implementar estas tecnologías para el desarrollo de la informatización de la sociedad.

POR TANTO: En el ejercicio de las facultades que me están conferidas,

RESUELVO:

PRIMERO: Autorizar la instalación de los Sistemas de Comunicaciones de Banda Ancha por Líneas Eléctricas en interiores de edificios o complejos constructivos.

SEGUNDO: La importación de equipos y dispositivos auxiliares para los Sistemas de Comunicaciones de Banda Ancha por Líneas Eléctricas será autorizada por la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, en lo adelante la Agencia.

TERCERO: Las entidades debidamente autorizadas para la comercialización de medios de telecomunicaciones en el país, que deseen obtener un Permiso para importar y comercializar estos equipos y sus dispositivos auxiliares en el territorio nacional, deberán presentar su solicitud a la Agencia, indicando de la entidad en cuestión los detalles relativos a su Objeto Social, documento que acredite su facultad para realizar esta actividad; debiendo además presentar por escrito su compromiso a cumplir con todas las disposiciones que se establecen por medio de la presente, abonando la suma de 500.00 CUP o CUC según corresponda, por la obtención del correspondiente Permiso que será expedido por un periodo de cuatro años y podrá ser renovado sujeto al pago de los correspondientes derechos.

CUARTO: Los equipos y dispositivos auxiliares que componen estos sistemas están sujetos, previo a su importación o comercialización, a la obtención de un Certificado de Aceptación Técnica otorgado por la Agencia por un término de dos años, y deben ser sometidos a los procedimientos de medición y comprobación técnica de sus parámetros por los laboratorios que designe ésta y puede emplear los

criterios que considere necesarios, para la realización de las mediciones de las señales con vistas a determinar la aceptación de los sistemas. En todos los casos, los gastos en que se incurra, producto del proceso de aceptación técnica, deben ser sufragados por la entidad que realiza la solicitud.

QUINTO: Para la utilización o prueba de los Equipos de Comunicaciones de Banda Ancha por Líneas Eléctricas, se deberá solicitar y obtener una autorización emitida por la Agencia, quien las registra y que debe contener, como mínimo, los siguientes datos:

a) Nombre del proveedor de infraestructura de redes propias de área local o de campo que instalará el acceso a Comunicaciones de Banda Ancha por Líneas Eléctricas, incluyendo número de teléfono y dirección electrónica de su representante para facilitar la solución de cualquier queja o interferencia.
b) Número de la inscripción expedida por la Agencia para operar la Red Propia donde serán utilizados los sistemas de Comunicaciones de Banda Ancha por Líneas Eléctricas.
c) Frecuencias de funcionamiento.
d) Fabricante, modelo y nombre comercial del equipamiento utilizado.
e) Número del Certificado de Aceptación Técnica para el modelo de equipo en cuestión, expedido por parte de la Agencia.
f) Ubicación de la instalación.
g) Proveedor del Servicio Público de Acceso a Internet (ISP) a la red en la cual se inserta el Sistema de Comunicaciones de Banda Ancha por Líneas Eléctricas.

SEXTO: Estos sistemas en su rango de frecuencia de trabajo tienen atribución secundaria, y no pueden reclamar protección procedente de las emisiones de otros sistemas y dispositivos de radiocomunicaciones, ni de las radiaciones que puedan originarse por equipos reconocidos para operar en la misma banda de frecuencias.

SÉPTIMO: Su utilización no puede causar interferencia perjudicial a las estaciones de otros sistemas de comunicaciones, que se hayan autorizado a operar con asignaciones de frecuencias, segmentos o bloques de frecuencias específicas en esta banda. En caso de interferencias con otros sistemas o equipos de telecomunicaciones, deben eliminarse dichas interferencias y en caso de persistir las mismas deben desconectarse.

OCTAVO: Se faculta a la Agencia para determinar cuáles son los lugares, zonas o regiones excluidas de la instalación de los Equipos de Comunicaciones de Banda Ancha por Líneas Eléctricas, como protección a otros sistemas de radiocomunicaciones que por su importancia lo requieran.

NOVENO: El resultado de las pruebas de instalación y aceptación, así como la comprobación de los niveles de radiación de los sistemas instalados de los Sistemas de Comunicaciones de Banda Ancha por Líneas Eléctricas deben de informarse a la Agencia para su evaluación.

DÉCIMO: Los suministradores de la tecnología deben contar con los medios técnicos para di- chas pruebas y comprobaciones, teniendo la Agencia el derecho de participar en dichas pruebas según su

criterio, así como en las comprobaciones por quejas de afectaciones a otros servicios. Los gastos de la Agencia en el caso de comprobaciones por quejas de afectaciones a otros servicios deberán asumirse por el suministrador.

En los anexos I y II de la presente Resolución y que forman parte integrante de la misma, se relacionan las especificaciones generales que deben cumplir los Sistemas de Comunicaciones de Banda Ancha por Líneas Eléctricas para su introducción en el país, así como los valores límites de señales radiadas en exteriores y radiadas en interiores permitidos.

DÉCIMO PRIMERO: El incumplimiento de lo dispuesto en la presente, puede implicar el retiro temporal o permanente de la Autorización o Licencia inicialmente otorgada, la desconexión de la red, así como la invalidez del infractor para el establecimiento futuro de otra red o sistema conforme a la presente regulación, sin prejuicio de la adopción de cualquier medida o sanción aplicable conforme con las disposiciones legales vigentes en la materia.

DÉCIMO SEGUNDO: Facultar a la Dirección de Regulaciones y Normas del Ministerio de la Informática y las Comunicaciones para realizar en lo sucesivo, la actualización de lo dispuesto en la presente Resolución, según el desarrollo de la tecnología y asegurar la satisfacción apropiada de las necesidades de empleo de estos sistemas.

DÉCIMO TERCERO: Encargar a la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, la elaboración de los procedimientos para los trámites de solicitudes relacionadas con la presente Resolución, y la adopción de otras medidas pertinentes para garantizar el cumplimiento de lo dispuesto.

COMUNÍQUESE a los Viceministros, a la Dirección de Regulaciones y Normas, a la Agencia de Control y Supervisión del Ministerio de Informática y las Comunicaciones, a la Empresa de Telecomunicaciones de Cuba S.A., al Ministerio de la Industria Básica, a las entidades autorizadas en el país para comercializar equipos y medios de telecomunicaciones y a cuantas más personas naturales o jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

Dada en La Habana, a los 17 días del mes de diciembre del 2007.

Boris Moreno Cordovés
Ministro p.s.r.

ANEXO I

ESPECIFICACIONES GENERALES QUE DEBERÁN CUMPLIR LOS SISTEMAS DE COMUNICACIONES DE BANDA ANCHA POR LÍNEAS ELÉCTRICAS PARA SU INTRODUCCIÓN EN EL PAÍS

Características Técnicas a cumplir por el equipamiento PLC:

1- Operará con el tipo de modulación OFDM y permitirá la supresión de portadoras y la atenuación de las mismas para ajustar la máscara de potencia acorde al lugar de instalación con el objetivo de no perturbar a los clientes licenciados en el área que trabajen en la misma Banda de Frecuencia del sistema PLC.
2- La Banda de Frecuencia permitida será entre 2 a 30 MHz. contando el sistema con más de 1500 portadoras en cada uno de los Modos de Trabajo.
3- Se podrá trabajar en Modulación por división en Frecuencia y en Modulación por División en Tiempo empleándose selectivamente Modos de trabajo con anchos de Banda de 10, 20 y 30 MHz, alcanzándose velocidades de hasta 200 Mbps.
4- Los sistemas deben permitir su evolución para la implementación del IPV6.
5- La densidad de la potencia espectral de la señal inyectada debe ser un parámetro programable y su nivel no superará los -50 dBm/Hz con el empleo de acopladores capacitivos e inductivos acorde al medio de inyección de la señal.
6- El Nivel de Potencia Transmitida también debe ser un parámetro programable y debe estar en los órdenes de -70 dBm hasta los 10 dBm.
7- El equipo PLC debe poseer Controles Automáticos de Ganancia, los cuales podrán ser deshabilitado para el control manual de la misma.
8- Se tendrán que instalar los filtros especificados por el suministrador para evitar fugas hacia la Red Eléctrica Pública de la señal PLC.
9- Es requisito fundamental compatibilizar las bandas o frecuencias específicas a suprimir para cada una de las instalaciones que se propongan realizar.

ANEXO II

ESPECIFICACIONES DE LOS VALORES LÍMITES DE SEÑALES PERMITIDOS EN LOS SISTEMAS DE COMUNICACIONES DE BANDA ANCHA POR LÍNEAS ELÉCTRICAS. RADIADAS EN EXTERIORES Y RADIADAS EN INTERIORES.

Límites de señales conducidas por la línea eléctrica

En los puntos de conexión a la red eléctrica pública los niveles máximos promedio de voltajes procedentes de las señales de radiofrecuencia de los Sistemas de Comunicaciones de Banda Ancha por Líneas Eléctricas, medidos desde cada conductor respecto a tierra mediante una red estabilizadora de impedancia (50 µH/50Ω), no podrán sobrepasar los siguientes valores:

1) Para señales de frecuencias menores de 2000 KHz. - 1 000 µV (60 dB/µV)
2) Para señales de frecuencias entre 2 000 y 30 000 kHz - 3000 µV (69.54 dB/µV)
3) Para señales de frecuencias mayores de 30 000 KHz - 250 µV (48 dB/µV)

Límites de señales radiadas en exteriores:

a) En puntos exteriores al edificio en que se encuentre instalada la red PLC, para frecuencias inferiores a 2 000 KHz. midiendo a una distancia de 30 m, la intensidad de campo promedio no podrá sobrepasar 25 µV /m. (28 dB/µV).
b) En puntos exteriores al edificio en que se encuentre instalada la red PLC, para frecuencias superiores a 2 000 KHz. e inferiores a 30 000 KHz a una distancia de 30 metros, la intensidad de campo promedio no podrá sobrepasar 100 µV /m. (40 dB/µV)
c) En puntos exteriores al edificio en que se encuentre instalada la red PLC, para frecuencias superiores a 30 000 KHz. a una distancia de 3 metros, la intensidad de campo promedio no podrá sobrepasar 100 µV/m. (40 dB/µV)

Límites de señales radiadas en interiores:

a) Para cualquier frecuencia utilizada por la red PLC, la intensidad de campo promedio no podrá sobrepasar los 7 V/m (137 dB/µV) en aquellos lugares donde se encuentren personas.
b) La potencia máxima de salida promedio de los equipos PLC no podrá superar los 20 mW de potencia promedio.

RESOLUCIÓN No. 141/2007

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000 cambió la denominación del Ministerio de Comunicaciones por el de Ministerio de la Informática y las Comunicaciones, para que desarrollara las tareas y funciones que realizaba el Ministerio de Comunicaciones así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sideromecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 30 de agosto del 2006, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: El Acuerdo No. 2817 de fecha 25 de noviembre de 1994, adoptado por el Comité Ejecutivo del Consejo de Ministros, faculta a los Jefes de los Organismos de la Administración Central del Estado; dictar en el límite de sus facultades y competencia, reglamentos, resoluciones y otras

disposiciones de obligatorio cumplimiento para el sistema del organismo; y en su caso , para los demás organismos, órganos locales del Poder Popular, las entidades estatales, el sector cooperativo, mixto, privado y la población.

POR CUANTO: El Acuerdo No. 3736, de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo del Consejo de Ministros, establece que el Ministerio de la Informática y las Comunicaciones en lo adelante MIC es el organismo encargado de ordenar, regular y controlar los servicios informáticos, de telecomunicaciones y postales, nacionales e internacionales y otros servicios afines en los límites del territorio nacional, así como, de conjunto con las organizaciones correspondientes, el acceso a las redes de infocomunicaciones con alcance global. Establece además que es el organismo encargado de la gestión de los recursos comunes y escasos en materia de dichos servicios, así como de proponer y controlar las prioridades para la implementación de estos.

POR CUANTO: Los Organismos Internacionales que hoy operan los Recursos de Internet han ido ganando en organización, atendiendo a los cambios de innovaciones tecnológicas que se están dando a escala mundial, lo que les ha permitido una mayor regulación y control de las políticas que hoy la rigen.

POR CUANTO: Nuestro país debe crear las condiciones necesarias para adecuar, coordinar y regular las políticas que rigen Internet, de manera tal que se logre una efectiva organización y funcionamiento de las Redes Telemáticas en el país que operan esos Recursos de Internet, teniendo en cuenta que su correcto funcionamiento es importante para el desarrollo económico y social del país.

POR CUANTO: La Empresa de Tecnologías de la Información y Servicios Telemáticos (CITMATEL) del Ministerio de Ciencias y Tecnología y Medio Ambiente, opera el CUBANIC y los servidores primarios y secundarios del punto cu (.cu) desde la primera conexión de Cuba a Internet.

POR CUANTO: Se ha establecido la responsabilidad legal del CUBANIC, como Centro que garantiza la administración y gestión del dominio geográfico punto cu (.cu) el funcionamiento de los servidores primarios y secundarios, el Registro de Nombres de Dominios de Segundo Nivel bajo el .cu y las categorías de dominios genéricas que operaran bajo él.

POR CUANTO: Resulta necesario oficializar la entidad que opera el CUBANIC de la República de Cuba.

POR TANTO: En el ejercicio de las facultades que me están conferidas.

RESUELVO:

ÚNICO: Designar a la Empresa de Tecnologías de la Información y Servicios Telemáticos (CITMATEL) del Ministerio de Ciencias, Tecnologías y Medio Ambiente, como el operador oficial del CUBANIC, Centro que garantiza la administración y gestión del dominio geográfico punto cu (.cu), del funcionamiento de los servidores primarios y secundarios y del Registro de Nombres de Dominios de Segundo Nivel bajo el .cu y las categorías de dominios genéricas que operara bajo él.

COMUNÍQUESE al Ministerio de Ciencia Tecnología y Medio Ambiente, a los Viceministros del MIC, a la Dirección de Regulaciones y Normas, a la Agencia de Control y Supervisión, a la Empresa de Tecnologías de la Información y Servicios Telemáticos (CITMATEL) así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en la ciudad de La Habana, a los días 4 del mes de Septiembre del 2007.

Ramiro Valdés Menéndez
Ministro

3. PROVEEDORES DE SERVICIOS

RESOLUCIÓN No. 132/2021

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros, de 22 de mayo de 2017, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de estos.

POR CUANTO: Las Resoluciones 256 y 257, de 29 de septiembre de 2017, del Ministro de Comunicaciones, regulan la organización, funcionamiento y expedición de la licencia de operación del proveedor de servicios públicos de aplicaciones y aprueban las definiciones y alcance de los servicios que brindan los proveedores de Servicios del Entorno Internet, respectivamente, las cuales resultan ineficaces en la actualidad, debido al desarrollo y actualización del marco regulatorio de las Tecnologías de la Información y la Comunicación en el país.

POR TANTO: En el ejercicio de las atribuciones conferidas en el Artículo 145 inciso d), de la Constitución de la República de Cuba;

RESUELVO

ÚNICO: Derogar las Resoluciones siguientes:

1. Resolución 256, de 29 de septiembre de 2017, del Ministro de Comunicaciones, que regula la organización, funcionamiento y expedición de la licencia de operación del proveedor de servicios públicos de aplicaciones.

2. Resolución 257, de 29 de septiembre de 2017, del Ministro de Comunicaciones, aprueba las definiciones y alcance de los servicios que brindan los proveedores de Servicios del Entorno Internet.

COMUNÍQUESE a los viceministros, a los directores generales de Informática y de Comunicaciones, y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y a los directores territoriales de control, a los directores de Inspección y de Regulaciones, todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los 14 días del mes de octubre de 2021.

Mayra Arevich Marín

RESOLUCIÓN No. 127/2019

POR CUANTO: El Acuerdo 8151, del 22 de mayo de 2017, del Consejo de Ministros, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y su implementación.

POR CUANTO: Las resoluciones 55 y 104 del Ministro de la Informática y las Comunicaciones, actualmente de Comunicaciones, del 9 de marzo de 2009 y del 16 de junio del 2011, respectivamente, regulan la organización, el funcionamiento, registro y expedición de licencias de operación para los proveedores de servicios públicos de Alojamiento, Hospedaje y Aplicaciones, y con las exigencias del desarrollo alcanzado en las Tecnologías de la Información y la Comunicación, los servicios y el uso racional de los recursos, se hace necesario actualizar las referidas normas jurídicas y en consecuencia derogar estas.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO DEL PROVEEDOR DE SERVICIOS PÚBLICOS DE ALOJAMIENTO Y DE HOSPEDAJE EN EL ENTORNO INTERNET

CAPÍTULO I
OBJETO, DEFINICIONES Y ALCANCE

Artículo 1. El objeto del presente Reglamento es establecer las normas para la organización, funcionamiento y expedición de licencias de operación del proveedor de servicios públicos de alojamiento y de hospedaje en el entorno Internet en el territorio nacional.

Artículo 2. El presente Reglamento se aplica a la persona jurídica que haya solicitado y reciba la licencia de operación del Ministerio de Comunicaciones, para brindar los servicios de alojamiento o de hospedaje o ambos.

Artículo 3. El proveedor de servicios públicos de alojamiento y de hospedaje en el entorno Internet, en lo adelante el proveedor, puede prestar servicios clasificados como:

a) De alojamiento, gestión y colocación de servidores;
b) de hospedaje de sitios, aplicaciones e información.

Artículo 4. El proveedor soporta sus servicios con alcance nacional e internacional sobre las redes públicas de telecomunicaciones, en correspondencia con la legislación vigente.

CAPÍTULO II
DE LA LICENCIA DE OPERACIÓN

Artículo 5. La condición de proveedor se otorga mediante aprobación y expedición de la licencia de operación, para lo que el aspirante realiza la solicitud a la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones, en lo adelante UPTCER.

Artículo 6. La UPTCER es la encargada de la expedición, modificación o renovación de la licencia de operación de proveedor y su inscripción en el Control Administrativo Central Interno del Ministerio de Comunicaciones; para las solicitudes que reúnan los requisitos establecidos y sean aceptadas, la UPTCER dispone de hasta treinta días hábiles a los fines de entregar la licencia de operación e igual plazo para notificar a los no aceptados.

Artículo 7. Se exceptúan de realizar la solicitud al Ministerio de Comunicaciones aquellos proveedores designados para prestar servicios públicos de acceso a Internet y los que se hayan autorizado por este Ministerio como proveedores públicos de alojamiento, hospedaje y aplicaciones, con anterioridad a la fecha de aprobación de este Reglamento.

Artículo 8. La solicitud debe ir acompañada de los documentos siguientes:

a) Carta del aspirante en la que se declare los datos generales de la entidad;
b) copia certificada del poder o resolución de designación del representante legal de la entidad;
c) documento que informe los aspectos técnicos del servicio, el equipamiento disponible y los programas y aplicaciones informáticas que utiliza;
d) dictamen sobre la seguridad de las Tecnologías de la Información y la Comunicación; y
e) otros documentos de interés que se soliciten por la UPTCER como requisito adicional a lo regulado por el presente Reglamento.

Los datos declarados en los documentos presentados pueden ser objeto de comprobación por los inspectores de las oficinas territoriales de Control del Ministerio de Comunicaciones.

Artículo 9. A partir de la solicitud presentada, la UPTCER entrega, de acuerdo con la condición otorgada los documentos siguientes:

a) Una licencia de operación, si fuere el solicitante un nuevo proveedor de servicios;
b) una modificación o renovación de la licencia de operación, si ya se le hubiere otorgado tal condición.

Artículo 10.1. La licencia de operación tiene un plazo de vigencia de cinco años; cualquier modificación en los parámetros informados en el Control Administrativo Central Interno del Ministerio de Comunicaciones, se comunica a la UPTCER por el representante legal de la entidad;

2. En la licencia de operación que se entregue se determina su nuevo término de duración, sobre la base de los datos aportados en las solicitudes de modificación.

Artículo 11. La licencia de operación se renueva dentro de los sesenta días antes del vencimiento del plazo de vigencia, mediante la presentación del documento de solicitud de renovación; una vez vencido el plazo de autorización, la entidad no puede brindar el servicio, y su representante legal está obligado a realizar todos los trámites como una nueva solicitud.

Artículo 12. El proveedor presenta la renuncia a su condición por escrito ante la UPTCER, con noventa días de antelación a la fecha en que se pretende que surta efectos.

Artículo 13. Constituyen causas para cancelar la licencia de operación por parte de la UPTCER, las siguientes:

a) El vencimiento del plazo por el que fue otorgada la licencia sin haberse solicitado su renovación;
b) el incumplimiento de lo establecido en el presente Reglamento, la legislación sobre telecomunicaciones, y las relacionadas con los servicios sobre internet y su seguridad;
c) la renuncia por parte del proveedor;
d) la extinción de la entidad a la que se le otorgó la licencia;

e) la cesión o el gravamen a favor de un tercero, en todo o en parte, de los derechos que son objeto de la licencia de operación otorgada; y
f) las demás que correspondan, según la legislación vigente.

Artículo 14. Los proveedores abonan por los derechos de licencia de operación de los servicios la cantidad de trescientos pesos cubanos por la licencia, y ciento cincuenta pesos cubanos por la renovación o modificación; el pago se realiza directamente en la sucursal bancaria según establece la legislación vigente del Ministerio de Finanzas y Precios y presentan el comprobante de pago a la UPTCER para la obtención de la licencia, quien anexa la copia de este al expediente.

CAPÍTULO III
DE LAS NORMAS TÉCNICAS, LA HOMOLOGACIÓN Y LOS ACUERDOS DE NIVEL DE SERVICIOS

Artículo 15. Las normas técnicas aplicables a la infraestructura sobre la que se soportan los servicios de un proveedor son las establecidas de acuerdo con la legislación vigente, de conformidad con las recomendaciones de la Unión Internacional de Telecomunicaciones o de otros organismos internacionales, y de los tratados de los que la República de Cuba sea Estado parte.

Artículo 16. El proveedor está obligado a cumplir las especificaciones de los puntos de conexión de los servicios de soporte que utilice; las interfaces entre los puntos de interconexión y la red del proveedor están normalizadas y se procura, siempre que sea posible, utilizar las más avanzadas técnicamente.

Artículo 17. Los equipos que se conecten a las redes públicas de telecomunicaciones o hagan uso del espectro radioeléctrico para la prestación del servicio, deben estar homologados según lo establecido y cumplir las disposiciones vigentes sobre el empleo del espectro radioeléctrico en el país.

Artículo 18. Los proveedores establecen en sus contratos con los proveedores de servicios de red, los indicadores de calidad que definan y garanticen los parámetros de estos, el cumplimiento de las recomendaciones internacionales y las regulaciones nacionales vigentes, así como aquellas que las partes acuerden complementariamente.

Artículo 19. Las partes acuerdan según las regulaciones vigentes, entre otros indicadores y parámetros de calidad de servicio, los siguientes:

a) Los tipos de medición de los niveles de calidad que hacen de manera independiente y la periodicidad de la medición de cada indicador;
b) las condiciones bajo las cuales existe intercambio de información sobre estos indicadores;
c) los medios empleados para el intercambio de la información;
d) los períodos dentro de los cuales se acepta por la otra parte la calificación que se haga de los mencionados niveles de servicio.

CAPÍTULO IV
DE LAS OBLIGACIONES DE LOS PROVEEDORES

Artículo 20. El proveedor al prestar servicios de alojamiento y de hospedaje garantiza las condiciones técnicas mínimas siguientes:

a) Sistema de almacenamiento conectado a la red, conocido como SAN;
b) local con condiciones apropiadas;
c) sistema de climatización redundante;
d) alimentación eléctrica estable, confiable y permanente;
e) grupo electrógeno de respaldo de energía;
f) sistema de detección de incendios;
g) sistema de aterramiento;
h) sistemas de seguridad física y lógica;
i) control de acceso al servicio;
j) monitorización sistemática;
k) registro bajo el dominio .cu en el CUBANIC;
l) sistema de respaldo de la información, backup, y de recuperación ante desastres.

Artículo 21. El proveedor tiene las obligaciones siguientes:

a) Utilizar los servicios portadores, finales o de difusión existentes en la red pública de telecomunicaciones, sin vulnerar las concesiones administrativas otorgadas de servicios públicos de telecomunicaciones;
b) admitir como clientes del servicio a todas las personas naturales o jurídicas que lo deseen, siempre que tenga capacidades disponibles;
c) garantizar la administración, operación y seguridad de la información de los servicios que presta, de acuerdo con lo establecido en el marco jurídico existente;
d) adoptar las medidas necesarias para garantizar el cumplimiento de los principios de:
    i. salvaguarda del orden público y la defensa del país;
    ii. no discriminación; y
    iii. protección de la juventud y de la infancia.
e) garantizar, en lo que le corresponde, la seguridad de las Tecnologías de la Información y la Comunicación en la red que utilice;
f) adquirir tecnología que permita el empleo de técnicas de virtualización para la optimización y uso eficiente de los recursos disponibles y brindar servicios soportados en la nube;
g) cumplir los requisitos técnicos del servicio que le sirve de soporte, incluidos los puntos de conexión, así como lo estipulado en las condiciones de interconexión contenidas en el Reglamento correspondiente y para el uso del espectro radioeléctrico;
h) sistematizar la gestión de vulnerabilidades, versiones y actualizaciones, parches, de las aplicaciones, software y firmware, sobre la base de la publicación de alertas de los fabricantes y la vigilancia tecnológica;
i) implementar las medidas y herramientas que garanticen la seguridad de las infraestructuras de la red y la detección e investigación de incidentes de seguridad;

j) cumplir las disposiciones establecidas por los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, ante situaciones excepcionales;
k) reportar los incidentes de seguridad informática que se detecten por las vías y procedimientos establecidos en la legislación vigente;
l) cumplir con calidad el servicio contratado con sus clientes;
m) brindar en línea a sus clientes, la información sobre el uso de los servicios;
n) mantener informados a los clientes de las características, bondades, tarifas a aplicar y otras cuestiones relacionadas con el servicio ofertado; detallar las características y alcance del servicio que presta en los contratos a suscribir y comunicar cualquier modificación de este con una antelación de treinta días;
o) mantener el principio de inviolabilidad y secreto de las comunicaciones y de confidencialidad de los aspectos requeridos, de conformidad con lo dispuesto en la Constitución de la República y las normas dictadas al efecto;
p) establecer un sistema eficiente de recepción y solución de reclamaciones y quejas de los clientes por los servicios proporcionados;
q) permitir y facilitar la realización de inspecciones de los equipos, edificios e instalaciones relacionadas con el servicio autorizado que se indiquen por las oficinas territoriales de Control, por la Oficina de Seguridad para las Redes Informáticas ambas del Ministerio de Comunicaciones y por los demás órganos e instancias autorizados del país, sobre los documentos y los servicios en operación y el acceso a los equipos e instalaciones;
r) brindar las informaciones establecidas u otras que se solicite por el Ministerio de Comunicaciones;
s) garantizar a sus clientes de forma fácil la administración de los servicios contratados que lo requieran;
t) establecer en los contratos de servicios la exigencia del mantenimiento y soporte de las aplicaciones y servicios hospedados;
u) cumplir con la protección y tratamiento de los datos personales de sus clientes;
v) potenciar la capacitación del personal especializado que labora en esta área;
w) solicitar la licencia de proveedor de servicios públicos de aplicaciones a las personas que requieran este servicio de hospedaje;
x) priorizar los servicios de alojamiento a los sitios web a través de los cuales se brinden servicios públicos de información o de aplicaciones, entre los que se incluyen los sitios oficiales de los órganos del Estado y los organismos de la Administración Central del Estado, los proyectos nacionales de informatización y otros de interés nacional aprobados por el Ministerio de Comunicaciones.

Artículo 22. El proveedor cuando tenga conocimiento efectivo de acuerdo con lo dispuesto en el Artículo 25 de actividades ilegales o que violen los principios enunciados en el inciso d) del artículo anterior, está obligado a informar a las autoridades competentes y actuar con diligencia para evitar o poner fin a tales actividades.

Artículo 23. El proveedor cuando detecte vulnerabilidades que afectan la seguridad de la infraestructura tecnológica o que puedan propiciar la afectación de otros clientes hospedados o alojados por el propio

proveedor, o de la infraestructura de terceros países, debe gestionar su solución y, en dependencia del impacto, resolver el contrato con el cliente que la origina e informar a las autoridades competentes.

Artículo 24. El proveedor de un servicio consistente en almacenar contenidos de información que proporciona y actualiza el propio cliente, no es responsable por la información almacenada, siempre que:

a) No tenga conocimiento efectivo de que la actividad o la información almacenada es ilícita, violatoria de un principio, o de que lesiona bienes o derechos de un tercero susceptibles de indemnización; o que se demuestre la reclamación de la legitimidad de la violación del derecho de propiedad de algún artículo publicado en su sitio;
b) con el conocimiento efectivo de los hechos, actúe con diligencia para retirar la información o hacer imposible el acceso a ella, y poner en conocimiento de esta actuación al cliente del servicio de que se trate.

Artículo 25. El proveedor de servicios tiene conocimiento efectivo de que la actividad o la información almacenada es ilícita, violatoria de un principio, o que lesiona bienes o derechos de un tercero susceptibles de indemnización, cuando:

a) Un órgano competente haya declarado la ilicitud de los datos, orientado su retirada o que se imposibilite el acceso a estos;
b) haya recibido informe sobre la existencia de una infracción del marco regulatorio vigente.

Artículo 26. El proveedor es responsable de la información almacenada en su infraestructura cuando el cliente del servicio le contrate la gestión de esta.

Artículo 27. Los proveedores son responsables de coordinar entre sí la interconexión, sincronización y redundancia de sus centros de datos con el objetivo de garantizar la estabilidad y continuidad de los servicios.

CAPÍTULO V
DE LAS TARIFAS PARA LOS SERVICIOS

Artículo 28. El proveedor establece las tarifas de los servicios públicos de alojamiento y de hospedaje de conformidad con la legislación vigente en el país.

Artículo 29. El proveedor establece precios preferenciales en el pago de sus servicios, cuando los clientes hospedan proyectos de impacto nacional en la estrategia de informatización, determinados por la Dirección General de Informática.

CAPÍTULO VI
MEDIDAS Y PROCEDIMIENTOS A APLICAR ANTE INCUMPLIMIENTOS DEL PROVEEDOR

Artículo 30. El proveedor que incumpla lo dispuesto en el presente Reglamento y en las disposiciones legales vigentes en la materia, está sujeto a la aplicación de las medidas siguientes:

a) Notificación preventiva;
b) invalidación temporal o parcial o cancelación de las licencias de operación administrativamente entregadas por la UPTCER del Ministerio de Comunicaciones;
c) suspensión temporal o parcial o cancelación de los servicios que haya contratado con el proveedor de servicios públicos de transmisión de datos y acceso a Internet.

Artículo 31. El inspector de las oficinas territoriales de Control del Ministerio de Comunicaciones es la autoridad facultada para aplicar las medidas referidas en el artículo anterior e informar a la UPTCER sobre estas y la decisión acerca de su aplicación.

Artículo 32. El proveedor sujeto a la aplicación de las medidas descritas en el Artículo 30, puede apelar en primera instancia ante el Director de las oficinas territoriales de Control, en el plazo de diez días hábiles contados a partir de la fecha de su notificación, formular las alegaciones que considere oportunas y ofrecer las pruebas que estime convenientes; el Director de las oficinas territoriales de Control dispone de un plazo de treinta días hábiles para dar respuesta a partir de la presentación de la apelación.

Artículo 33. El proveedor que decida impugnar la medida impuesta en la primera instancia de reclamación, dispone de un plazo de diez días hábiles a partir de su notificación para solicitar una revisión ante el Director General de Informática, el que dispone de un plazo de treinta días hábiles, contados a partir del recibo oficial de la reclamación, para resolver lo que proceda; contra esta decisión no cabe otro recurso por vía administrativa.

Artículo 34. El proveedor que haya sido objeto de una medida por incumplimiento de sus obligaciones, una vez resuelto el expediente que dio lugar a esta, puede presentar una nueva solicitud de licencia de operación a la UPTCER, quien tiene en cuenta la información presentada y, una vez comprobada por los inspectores de las oficinas territoriales de Control la solución de las deficiencias detectadas, determina sobre el otorgamiento de la licencia.

SEGUNDO: El proveedor para solicitar, mantener o ampliar los servicios de conectividad presenta su licencia de operación al operador de servicios públicos de telecomunicaciones.

TERCERO: El Director General de la UPTCER queda responsabilizado con la elaboración de los procedimientos internos necesarios para el otorgamiento, renovación o modificación de las licencias de operación vigentes a la fecha de entrada en vigor de la presente.

DISPOSICIÓN FINAL

PRIMERA: Los proveedores de servicios públicos de alojamiento, hospedaje y aplicaciones, en un plazo de noventa días posteriores a la entrada en vigor de la presente, actualizan la información relativa a los parámetros de prestación del servicio, de acuerdo con lo que se dispone en este Reglamento, para su inscripción en el Control Administrativo Central Interno y que le sea entregada por la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico la licencia de operación como proveedor de servicios públicos de alojamiento y hospedaje.

SEGUNDA: Los directores generales de Informática, de Comunicaciones y de la UPTCER, y los directores de Inspección y de las oficinas territoriales de control del Ministerio de Comunicaciones, quedan encargados, según corresponda, del control del cumplimiento de lo que por la presente se dispone.

TERCERA: El glosario de términos y definiciones anexo forma parte del contenido de la presente Resolución.

CUARTA: Derogar las resoluciones 55, del 9 de marzo de 2009 y 104, del 16 de junio de 2011 del Ministro de la Informática y las Comunicaciones.

NOTIFÍQUESE a los directores generales de Informática, de Comunicaciones, y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y a los directores territoriales de control pertenecientes a este Ministerio, al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A., al Presidente del Grupo Empresarial de la Informática y las Comunicaciones y a los proveedores públicos de alojamiento, hospedaje y aplicaciones.

COMUNÍQUESE a los viceministros, a los directores de Inspección y de Regulaciones, al Director General de la Oficina de Seguridad para las Redes Informáticas, todos del Ministerio de Comunicaciones, así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los días 24 del mes de junio del 2019.

Jorge Luis Perdomo Di-Lella

ANEXO

GLOSARIO DE TÉRMINOS Y DEFINICIONES

1. **Almacenamiento Conectado a la Red (SAN del inglés Storage Area Networks):** capacidad de almacenamiento extra que puede solicitar un cliente que tiene un contrato de servidor dedicado, es decir, un servidor para su uso exclusivo, además puede ser empleado como complemento de otros servicios que se comercialicen.
2. **Alojamiento:** servicio de colocación, conexión, gestión y administración de equipos informáticos, consistente básicamente en vender o alquilar un espacio físico de un centro de datos, para que el cliente coloque su propio equipamiento.
3. **Hospedaje:** servicio de almacenamiento, conectividad y otros servicios dedicados al despliegue de la información que se quiera sea accesible por una red, que pueden ser desde un sitio de Internet, programas y las aplicaciones asociadas hasta la información de una red interna o Intranet.

4. **Licencia de operación:** autorización por la que se faculta a su tenedor para la operación de los servicios de alojamiento y hospedaje.
5. **Proveedor de servicios públicos de Aplicaciones:** persona jurídica o natural autorizada para comercializar servicios de aplicaciones a terceros y hace uso del entorno Internet, conocidos como ASP, por sus siglas en inglés.
6. **Proveedor de servicios públicos de acceso a Internet:** persona jurídica autorizada para prestar uno o varios tipos de servicios del entorno Internet, en todo el territorio nacional, conocidos como ISP, por sus siglas en inglés.

RESOLUCIÓN No. 99/2019

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros, de 22 de mayo de 2017, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de estos.

POR CUANTO: La experiencia acumulada en la aplicación de la Resolución 128 del Ministro de la Informática y las Comunicaciones, de 16 de agosto de 2011, que aprobó el Reglamento para las Redes Privadas de Datos, referida a personas jurídicas en calidad de titulares de las redes, y de la Instrucción 3 del Viceministro Primero de la Informática y las Comunicaciones, de 9 de septiembre del 2010 que establece el procedimiento de solicitud de autorización para la construcción de enlaces de fibra óptica en redes privadas, aconsejan su actualización para ampliar su alcance e incluir la titularidad a personas naturales y atemperarlas a las exigencias técnicas establecidas en materia de telecomunicaciones, por lo que es necesario emitir una nueva disposición normativa que derogue las referidas anteriormente.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el Artículo 145 inciso d), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO PARA LAS REDES PRIVADAS DE DATOS

CAPÍTULO I
OBJETO, GENERALIDADES Y LEGISLACIÓN APLICABLE

Artículo 1. El objeto del presente Reglamento es el establecimiento de las normas para la organización, funcionamiento y expedición de las licencias de operación de las redes privadas de datos.

Artículo 2. Los términos que se citan a continuación tienen el significado siguiente:

a) **Enlace transversal:** enlace de conectividad entre dos redes privadas de datos con licencias de operación independientes que permite la transmisión de la información entre ambas y que solo puede ser provista por el proveedor autorizado de servicios públicos de telecomunicaciones, previa autorización.
b) **Red privada de datos:** red de telecomunicaciones cuya infraestructura de red está instalada en una misma localidad o en distintas localidades geográficas e interconectadas entre sí por enlaces de telecomunicaciones, con el objetivo de satisfacer las necesidades de servicios de datos de su titular.
c) **Red privada virtual VPN:** tecnología de red que permite un enlace lógico seguro entre dos redes o dos puntos de una red privada de datos sobre una red pública de telecomunicaciones.
d) **Red pública de telecomunicaciones:** red de telecomunicaciones que se explota principalmente para prestar servicios públicos de telecomunicaciones y tecnologías de la información y la comunicación.
e) **Representante Legal del Titular:** persona natural designada a los efectos de ostentar la representación del titular.
f) **Titular:** persona a la que se le otorga la autorización por el Ministerio de Comunicaciones para brindar servicios privados de transmisión de datos a través de una red privada de telecomunicaciones.

Artículo 3. Las redes privadas de datos se soportan sobre las redes públicas de telecomunicaciones y por recursos propios.

Artículo 4. La operación, administración y provisión de servicios de las redes privadas tiene como objetivo satisfacer las necesidades de servicios de datos del titular de la red, en lo adelante el titular, y de los integrantes de esta; las que no pueden prestar servicios a terceros, salvo casos expresamente autorizados por este Ministerio.

Artículo 5. La responsabilidad que se derive de la operación, administración y de la prestación de dichos servicios es competencia del titular, o su representante legal; las redes cuyo titular es una persona natural se constituyen para dar servicios sin retribución económica.

Artículo 6. En el caso de que la red privada de datos corresponda a una persona jurídica y el representante legal del titular solicite servicios de conectividad al proveedor de servicios públicos y este no pueda garantizarlos, puede solicitar a la Dirección General de Comunicaciones del Ministerio de Comunicaciones, una autorización para la instalación de infraestructuras propias o solicitar a otros proveedores autorizados que satisfagan los servicios solicitados, que incluyen aquellos que utilizan el espectro radioeléctrico.

Artículo 7. La Dirección General de Comunicaciones decide en un plazo no mayor de treinta días hábiles a partir de recibir la solicitud, acerca de la autorización solicitada por el titular o su representante legal.

Artículo 8. Las solicitudes de construcción de enlaces de fibra óptica para el despliegue de infraestructura fuera de los límites de la propiedad para las redes privadas de personas jurídicas son presentadas por el representante legal del titular a la Dirección General de Comunicaciones, las que una vez recibidas, son sometidas a consulta interna con las instancias que se requiera según la envergadura de los proyectos, a fin de conciliar si procede la autorización correspondiente.

Artículo 9. De resultar positiva la respuesta, la Dirección General de Comunicaciones emite una Licencia de Ejecución de Obra al solicitante; de ser negativa la respuesta, la Dirección General de Comunicaciones emite documento que fundamente la decisión; se exceptúan de tramitar esta licencia a los titulares de redes privadas de personas jurídicas autorizados por la legislación vigente sobre el proceso inversionista.

Artículo 10. Las entidades constructoras de sistemas de fibras ópticas están obligadas a realizar la contratación y la ejecución de los trabajos de instalación solo con la presentación previa de la mencionada Licencia.

Artículo 11. El expediente a entregar por el solicitante contiene los documentos siguientes:

1. carta solicitud firmada por el titular o su representante legal, donde se argumenten los objetivos de la fibra a instalar y las limitantes para emplear otro tipo de enlace;
2. descripción de la traza que incluye la localización concreta de los puntos de conexión, y de las coordenadas si se trata de áreas rurales, así como el soporte a emplear y capacidad de hilos de la fibra;
3. esquema de la traza a partir de mapa planimétrico o topográfico según corresponda;
4. documento de conciliación con la Empresa de Telecomunicaciones de Cuba, S.A., donde se hagan constar por el representante de esa entidad la no disponibilidad de capacidades para satisfacer la demanda del solicitante en los lugares de referencia y la fecha en que esta podría satisfacerse, para el caso de que haya proyectos en tal sentido; igualmente se consignan los posibles intereses de la Empresa de Telecomunicaciones de Cuba, S.A., en el empleo de capacidades de la traza de referencia si se aprueba esta, para solucionar demandas no satisfechas en puntos de su recorrido;
5. documento de compatibilización con la Defensa, Seguridad y Orden Interior, donde se exprese su criterio sobre la inversión, que recoge además, los posibles intereses en el empleo de capacidades de la traza de referencia, si se aprueba esta;
6. constancia de que el interesado dispone de recursos técnicos y humanos para el servicio de mantenimiento posterior de los enlaces que instale, o de que existe una entidad especializada en disposición de prestarle dicho servicio, previa contratación.

Artículo 12. En los casos de necesidades de construcción de enlaces internos de fibra óptica para el despliegue de infraestructura dentro de los límites de la propiedad del titular no se requiere la presentación del expediente que se refiere en el artículo 11 de la presente Resolución.

Artículo 13. La entidad constructora al recibir una solicitud de contratación donde dude sobre si el área que abarca está o no dentro de los límites de la propiedad del titular, demanda del solicitante que

realice las consultas pertinentes a la Dirección General de Comunicaciones, a los fines de que esta dictamine si se requiere o no aplicar la entrega de la documentación referida. La Dirección General de Comunicaciones tiene un plazo de quince días para dar respuesta a la entidad constructora.

Artículo 14. Los titulares de las redes requieren tener la licencia entregada por las direcciones territoriales de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, en lo adelante direcciones territoriales de la UPTCER, para usar enlaces inalámbricos, y cumplen lo establecido según el marco regulatorio vigente.

Artículo 15. Los representantes legales de los titulares que son personas jurídicas, solicitan al proveedor de servicios públicos que le brinde los servicios de acceso a Internet desde sus domicilios a las personas naturales subordinadas que lo requieran por las funciones que realizan; dichos servicios de acceso a Internet otorgados se controlan administrativamente por el representante legal del titular.

Artículo 16. El titular se rige por el régimen jurídico específico que regula el uso del espectro radioeléctrico, las redes privadas de datos y por la legislación de telecomunicaciones de manera general.

CAPÍTULO II
DENOMINACIÓN DE LAS REDES PRIVADAS DE DATOS

Artículo 17. Las redes privadas de datos pueden denominarse a partir de su alcance geográfico, por los usuarios que la utilizan y por su grado de complejidad de la forma siguiente:

1. Por su alcance geográfico:

DENOMINACIÓN	DESCRIPCIÓN
REDES DE AREA PERSONAL PAN en inglés	Red de área personal empleada dentro del domicilio de una persona natural para la conexión de diferentes terminales ubicadas en la propiedad que habita.
REDES LOCALES LAN en inglés	Redes en las que el alcance geográfico se limita a un área donde el acceso a la red es controlado por el titular de esta.
REDES DE CAMPO CAN en inglés	Redes en las que el alcance geográfico abarca un complejo docente, hospitalario o industrial, cultural, científico u hotelero, entre otros, y está claramente delimitada su área por una demarcación perimetral y controlado por su titular el acceso al interior del recinto.
REDES TERRITORIALES MAN o WAN en inglés	Red de área geográfica amplia que conecta puntos de red distantes entre sí dentro o más allá del entorno de una ciudad.

2. Por los usuarios que la utilizan:

DENOMINACIÓN	DESCRIPCIÓN
REDES SECTORIALES	Redes que proporcionan conectividad a terminales para un determinado grupo, claramente delimitado, de entidades a uno o varios organismos de la Administración Central del Estado; así como a organizaciones políticas y de masas u otras organizaciones debidamente autorizadas y fuera de estos, no pueden suministrar conectividad a terceros.
REDES CORPORATIVAS O INSTITUCIONALES	Redes que proporcionan conectividad a terminales de empresas, Organizaciones Superiores de Dirección Empresarial, institutos, centros o asociaciones y entidades similares, claramente definidas por su personalidad jurídica propia y objeto social y que fuera de estas no suministran conectividad a terceros.

3. Por su grado de complejidad:

Se clasifican según lo establecido en la legislación vigente en materia de categorización de redes y de redes de condiciones especiales.

CAPÍTULO III
DEL OTORGAMIENTO, RENOVACIÓN Y MODIFICACIÓN DE LAS LICENCIAS

Artículo 18. Las redes privadas de datos requieren de la correspondiente licencia de operación entregada por las direcciones territoriales de la UPTCER. Se exceptúan de la licencia de operación las redes privadas de datos de área personal.

Artículo 19. **1** La licencia de operación para redes privadas de personas naturales limita su alcance geográfico a redes de área local, las cuales utilizan conexión inalámbrica y no exceden los cien mW de potencia radiada efectiva y en el supuesto de requerir conexión alámbrica, esta no puede atravesar la vía pública.

2. El tendido de los cables que se emplean fuera de los límites de las edificaciones se realiza de forma que:

a) no ocasionen problemas ambientales;
b) no atenten contra las regulaciones urbanísticas o no causen algún tipo de alteración al entorno;
c) no afecten el tránsito de las personas y vehículos.

Artículo 20. Las direcciones territoriales de la UPTCER, se encargan de la recepción de las solicitudes de otorgamiento, renovación o modificación de las licencias de operación de las redes; estas disponen de treinta días hábiles para entregar estas licencias, luego de aceptadas las solicitudes que cumplan los requisitos establecidos; las redes privadas de datos autorizadas se inscriben en el Control Administrativo Central Interno del Ministerio de Comunicaciones.

Artículo 21. Para solicitar la licencia de operación se suministra la información siguiente:

1) Datos generales del titular o su representante legal mediante disposición que lo faculta para ello.
2) Infraestructura y arquitectura de la red.
3) Alcance geográfico.
4) Descripción y esquema topológico de la red.

    a) Red de acceso.
    b) Red troncal, para personas jurídicas.
    c) Puntos de acceso a Internet.
    d) Centro de gestión o nodo principal de la red.

5) Tipos de servicios a brindar.
6) Equipamiento técnico para brindar los servicios.
7) Plataformas y programas informáticos con los que brindan los servicios.
8) Protocolos y algoritmos criptográficos que se emplean para la protección de la comunicación, que han sido autorizados por la autoridad competente.
9) Datos de equipamiento, frecuencia y puntos de conexión que se utilicen para enlaces inalámbricos autorizados por la Dirección General de Comunicaciones a través de las direcciones territoriales de la UPTCER, tanto troncales como de acceso.
10) Datos de contacto del personal de administración, de operación y de seguridad informática.
11) Cantidad máxima de usuarios según capacidad de la infraestructura instalada.
12) Nombre de dominios que tiene inscritos y declarar los que tengan en operación, para personas jurídicas.
13) Otros documentos de interés que se soliciten por la UPTCER como requisito adicional a lo regulado por el presente Reglamento.

Artículo 22. La licencia de operación implica la autorización para operar, administrar y brindar servicios por las redes por un plazo de dos años. El titular o su representante legal comunican a través de las direcciones territoriales de la UPTCER, cualquier modificación en los parámetros tanto de arquitectura como de servicios de la red informados, así como la existencia de redes privadas virtuales.

En la licencia de operación que se entregue se determina el nuevo término de duración de esta, sobre la base de los datos aportados en las solicitudes de modificación.

Artículo 23. 1. La licencia de operación expedida por las direcciones territoriales de la UPTCER para operar, administrar y brindar servicios a las redes se renueva antes de los sesenta días del vencimiento

del plazo de vigencia, mediante la presentación ante estas del documento de solicitud de licencia y el resto de los documentos exigidos según lo dispuesto en el artículo 21 del presente Reglamento.

2. Una vez transcurrido el plazo de vigencia y no sea gestionada la renovación, el titular o su representante legal no puede brindar el servicio y efectúa todos los trámites como una nueva inscripción.

Artículo 24. Los titulares de las redes por la inscripción abonan en la moneda que corresponda las cantidades siguientes:

1. redes locales de personas jurídicas, treinta pesos;
2. redes locales de personas naturales, diez pesos;
3. redes de campo, cien pesos;
4. redes territoriales, trescientos pesos.

Artículo 25. El titular o su representante legal, por los trámites de modificación o renovación abonan las cantidades siguientes:

1. redes locales de personas jurídicas, quince pesos;
2. redes locales de personas naturales, cinco pesos;
3. redes de campo, cincuenta pesos;
4. redes territoriales, ciento cincuenta pesos.

Estos pagos y los relativos al Artículo 24 se hacen directamente en la sucursal bancaria según establece la legislación vigente del Ministerio de Finanzas y Precios y se presenta el comprobante de pago a las direcciones territoriales de la UPTCER para la obtención de la licencia, cuya copia se anexa al expediente.

Artículo 26. Constituyen **causas** para retirar la licencia de operación por parte de la UPTCER las siguientes:

a) el vencimiento del plazo por el que fue otorgada la licencia sin haberse solicitado, en su caso, su renovación;
b) la invalidez de la licencia de operación por los inspectores de la Oficina Territorial de Control del Ministerio de Comunicaciones, cuando se produzcan, entre otras: incumplimientos de lo que se dispone en el presente Reglamento; de lo dispuesto en la legislación sobre telecomunicaciones en general y en específico las relacionadas con los Servicios sobre Internet y sobre la seguridad;
c) la disolución de la entidad licenciada;
d) las demás que correspondan de conformidad con lo legalmente establecido.

CAPÍTULO IV
DE LAS OBLIGACIONES EN CUANTO A LA ORGANIZACIÓN Y FUNCIONAMIENTO DE LOS PROVEEDORES

Artículo 27. Los titulares organizan y operan las redes a partir de los aspectos siguientes:

1. Para redes de personas jurídicas y naturales:

   a) presentar la licencia de operación recibida para solicitar los servicios del proveedor de servicios público de Acceso a Internet;
   b) garantizar la administración, operación, la provisión de los servicios y la seguridad y protección informática de su red de acuerdo con lo establecido en el régimen jurídico aplicable a los servicios de telecomunicaciones y en particular a los de transmisión de datos;
   c) reportar los incidentes de seguridad informática que se detecten por las vías y procedimientos establecidos en la legislación vigente;
   d) acatar las disposiciones establecidas por los órganos de la Defensa del país ante situaciones excepcionales, así como la realización de tareas impostergables para el aseguramiento de la Defensa, la Seguridad y el Orden Interior;
   e) permitir y facilitar la realización de las inspecciones de la infraestructura y los servicios que se brindan incluido el acceso a los equipos, domicilios, edificios e instalaciones relacionadas con la licencia de operación otorgada, que se indiquen por las direcciones territoriales de la UPTCER, la Oficina de Seguridad para las Redes Informáticas y de otras autoridades competentes;
   f) garantizar el principio de inviolabilidad y privacidad de las comunicaciones, salvo en los casos previstos por la ley, de conformidad con lo dispuesto en la Constitución de la República y la legislación vigente;
   g) asegurar la protección y tratamiento de los datos personales de sus usuarios;
   h) establecer en los contratos de servicios con sus usuarios la exigencia del mantenimiento y soporte de las aplicaciones y servicios hospedados;
   i) cumplimentar lo establecido en el marco jurídico vigente acerca de introducir, ejecutar, distribuir o conservar en los medios de cómputo programas y contenidos que puedan afectar la integridad y seguridad del país, así como información contraria al interés social, la moral y las buenas costumbres;
   j) brindar las informaciones periódicas establecidas u otras que se les demanden por el Ministerio de Comunicaciones;
   k) acceder en línea a la información sobre el uso y el tráfico del enlace contratado a su proveedor de servicios públicos de Acceso a Internet, a través del sitio web de dicho proveedor;
   l) tramitar la aprobación de la utilización de cualquier tipo de aplicación o servicio soportado que implique el uso de métodos de protección criptográfica de la información a transmitir;
   m) gestionar y controlar eficientemente el uso adecuado y tráfico de sus enlaces contratados al proveedor de servicios públicos de Acceso a Internet, así como de las direcciones IP reales que le han sido asignadas y la gestión y control de las direcciones IP ficticias;

n) exigir el cumplimiento de los indicadores de calidad del servicio contratado con su proveedor de servicios públicos de Acceso a Internet.

2. Para redes de personas jurídicas además de los aspectos anteriores:

a) implementar las medidas y herramientas que garanticen la seguridad y supervisión de la infraestructura de la red y la detección e investigación de incidentes de seguridad;
b) adquirir tecnología que permita el empleo de técnicas de virtualización para la optimización y uso eficiente de los recursos disponibles y brindar servicios soportados en la nube;
c) cumplir con las disposiciones vigentes sobre la seguridad y protección de la información oficial que sea introducida, transmitida o accedida;
d) poseer un Plan de Contingencia actualizado para la mitigación del impacto de los riesgos que afecten los servicios;

Las redes privadas de datos de personas jurídicas licenciadas como proveedores de Internet al Público, brindan estos servicios mediante enlaces exclusivos para ello.

3. Para redes de personas naturales además de los aspectos establecidos en el numeral 1:

a) garantizar el registro de los datos personales de los usuarios de la red que incluye el nombre, dirección, teléfono; los mecanismos de autenticación centralizado de los usuarios y los mecanismos de detección de tráfico de códigos malignos, a través de antivirus u otras soluciones equivalentes;
b) disponer del sistema conocido como antispam contra mensajes masivos dañinos en el uso del servicio interno de correo electrónico;
c) disponer de sistema para la detección de eventos de seguridad y almacenarlos, así como los detectados por los antivirus que faciliten la detección e investigación de incidentes;
d) cumplir con las disposiciones vigentes sobre la seguridad y protección de la información oficial; y velan que en las redes bajo su responsabilidad no sea introducida, transmitida o accedida esta;
e) provisión de servicio de acceso a internet solo bajo contrato con el proveedor de servicio público de acceso a Internet.

Artículo 28. Las redes privadas que tienen sitios web a través de los cuales brinden servicios públicos de información o de aplicaciones tienen que migrar estos a los centros de datos públicos, estos incluyen los sitios oficiales de los órganos superiores y locales del poder popular, de los órganos y organismos del Estado y el Gobierno y los sitios de los proyectos nacionales de informatización.

CAPÍTULO V
DE LA CONEXIÓN ENTRE LAS REDES

Artículo 29. Las redes privadas se conectan entre sí a través de los proveedores de servicios públicos de telecomunicaciones autorizados para ello.

Artículo 30. 1. La conexión entre redes privadas de personas jurídicas a través de enlaces transversales requiere de la aprobación de la dirección general de Informática y se otorga de manera excepcional, a partir de tener en cuenta intereses de carácter nacional.

2. Los titulares de redes presentan por intermedio del representante legal la correspondiente solicitud a través de las direcciones territoriales de la UPTCER.

Artículo 31. Los enlaces transversales autorizados se brindan por el proveedor de servicios públicos de telecomunicaciones autorizado para ello.

Artículo 32. Los titulares de las redes autorizadas a conectarse a través de enlaces transversales, adoptan las medidas pertinentes para evitar que una de ellas se convierta en proveedor de los servicios de la otra, diferentes a los que les fueron autorizados para el enlace.

CAPÍTULO VI
DE LAS NORMAS TÉCNICAS, LA HOMOLOGACIÓN Y LOS ACUERDOS DE NIVEL DE SERVICIOS

Artículo 33. Las normas técnicas aplicables a la infraestructura sobre la que se soporta una red, son establecidas en el país según la legislación vigente, de acuerdo con las recomendaciones de la Unión Internacional de Telecomunicaciones, o de otros organismos internacionales, de cuyos tratados Cuba sea Estado parte.

Artículo 34. Los titulares establecen dentro de sus contratos con el operador público de telecomunicaciones, los indicadores de calidad que definan y garanticen dichos servicios y que cumplan con las recomendaciones nacionales o internacionales que hayan sido establecidas por las regulaciones vigentes y por aquellas que las partes acuerden complementariamente.

Artículo 35. Los indicadores de calidad del servicio acordados por las partes precisan los tipos de medición de los niveles de calidad que hacen de manera independiente, la periodicidad de la medición de cada indicador, las condiciones bajo las cuales existe intercambio de información sobre estos, los medios empleados para el intercambio de la información y los períodos dentro de los cuales se acepta por la otra parte la calificación que se hace de los mencionados niveles de servicio.

Artículo 36. Los equipos de telecomunicaciones y de las tecnologías de la información y la comunicación que las redes privadas conecten a las redes públicas de telecomunicaciones o que hagan uso del espectro radioeléctrico tienen que haber obtenido previamente el correspondiente Certificado de

Homologación según lo establecido en las normativas vigentes; el incumplimiento de ello, impide la obtención de servicios del operador público de telecomunicaciones.

CAPÍTULO VII
MEDIDAS ANTE LOS INCUMPLIMIENTOS

Artículo 37. El incumplimiento de lo dispuesto por el presente reglamento está sujeto a la aplicación de las medidas siguientes:

a) notificación preventiva;
b) invalidación temporal o cancelación de las licencias de operación administrativamente concedidas al titular;
c) suspensión temporal o cancelación de los servicios y los contratos que el titular o su representante legal haya suscrito con el proveedor de servicios públicos de acceso a Internet;
d) el decomiso de los medios, instrumentos, equipamientos y otros, utilizados para cometer la infracción; así como de los efectos de la infracción, según proceda;
e) la aplicación de otras medidas que correspondan, de conformidad con el marco jurídico establecido en el país.

Artículo 38. El inspector de la Oficina Territorial de Control es la autoridad facultada para aplicar las medidas referidas en el artículo anterior e informar a la UPTCER sobre la medida impuesta y la decisión acerca de su aplicación.

Artículo 39. El titular o su representante legal sujeto a la aplicación de las medidas descritas anteriormente, puede apelar en primera instancia ante el director territorial de control, en un plazo de diez días hábiles contados a partir de la fecha de notificada la medida, y formulan las alegaciones y proponer las pruebas que crea convenientes a su derecho; a su vez el director territorial de control dispone de treinta días hábiles a partir de recibida la apelación para dar respuesta a dicha reclamación.

Artículo 40. El titular o su representante legal que desee impugnar la decisión de la primera instancia de apelación, dispone de diez días hábiles a partir de la notificación de esta, para presentarla ante el director general de Informática del Ministerio de Comunicaciones, quien dispone de sesenta días hábiles para dar respuesta, a partir de recibida la impugnación de la decisión de la apelación en la primera instancia; contra la decisión de esta instancia no cabe otro recurso en lo administrativo.

Artículo 41. El titular que ha sido objeto de una medida que motive la cancelación de la licencia de operación puede, resuelta las causas que dieron lugar a la medida impuesta, volver a presentar a las direcciones territoriales de la UPTCER su solicitud de inscripción, se toma en cuenta la información presentada y comprobada por los inspectores de la Oficina Territorial de Control de la solución de las deficiencias detectadas y determina sobre el otorgamiento de la nueva licencia de operación.

SEGUNDO: Las entidades legalmente establecidas y que se encuentran reconocidas para la comercialización de infraestructuras de telecomunicaciones a las redes en el territorio nacional, antes de satisfacer cualquier solicitud para el establecimiento de infraestructuras por medios propios de redes

privadas o para la comercialización de estas, solicitan al titular de la red, la presentación de la autorización correspondiente expedida por el Ministerio de Comunicaciones.

TERCERO: El director General de Comunicaciones queda encargado con la elaboración de los procedimientos necesarios para la implementación de lo dispuesto en la presente en un plazo de sesenta días posteriores a su publicación en la Gaceta Oficial de la República de Cuba.

CUARTO: Los titulares de las redes privadas de los órganos de la Seguridad y Defensa Nacional y Orden Interior quedan exceptuados del cumplimiento de lo establecido en el presente Reglamento y quedan sujetos a lo dispuesto en sus normas jurídicas.

QUINTO: Los directores generales de Informática, de Comunicaciones y de la UPTCER, el director de Inspección y los directores territoriales de control del Ministerio de Comunicaciones, quedan encargados según corresponda, del control del cumplimiento de lo que por la presente Resolución se dispone.

DISPOSICIONES FINALES

PRIMERA: Derogar la Resolución 128 del Ministro de la Informática y las Comunicaciones, de 16 de agosto de 2011, y la Instrucción 3 del Viceministro Primero de la Informática y las Comunicaciones, de 9 de septiembre del 2010.

SEGUNDA: La presente Resolución entra en vigor a los sesenta días posteriores a su fecha de publicación en la Gaceta Oficial de la República de Cuba.

DÉSE CUENTA a los jefes de los órganos del Estado y de los organismos de la Administración Central del Estado.

NOTIFÍQUESE a los directores generales de Informática, de Comunicaciones y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, a los directores territoriales de control pertenecientes al Ministerio de Comunicaciones, al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A. y al Presidente del Grupo Empresarial de la Informática y las Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de la Oficina de Seguridad para las Redes Informáticas, a los directores de Inspección y de Regulaciones, pertenecientes todos al Ministerio de Comunicaciones.

ARCHÍVESE el original en la dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 21 días del mes de mayo de 2019.

Jorge Luis Perdomo Di-Lella

RESOLUCIÓN No. 255/2017

POR CUANTO: El Acuerdo No. 8151 del Consejo de Ministros, de fecha 22 de mayo de 2017, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de estos.

POR CUANTO: Mediante la Resolución No. 179, de fecha 7 de octubre de 2008 y la Resolución No. 102, de fecha 16 de junio de 2011, ambas del Ministro de la Informática y las Comunicaciones, se aprobó el Reglamento para los Proveedores de Servicios de Acceso a Internet al Público, y se establecieron modificaciones, las cuales resulta necesario actualizar de acuerdo con las exigencias del desarrollo alcanzado en las Tecnologías de la Información y la Comunicación, los servicios y el uso racional de los recursos.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el inciso a), del Artículo 100 de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO DEL PROVEEDOR DE SERVICIOS DE ACCESO A INTERNET AL PÚBLICO

CAPÍTULO I
OBJETO, DEFINICIONES Y ALCANCE

Artículo 1. El objeto del presente Reglamento es establecer las normas para la organización, funcionamiento y expedición de la licencia de operación del Proveedor de Servicios de Acceso a Internet al Público, en lo adelante proveedor.

Artículo 2. A los efectos del presente Reglamento, los términos que se citan a continuación tienen el siguiente significado:

a) **Áreas de Internet:** espacios cerrados o abiertos, techados o al aire libre, alambrados o no, donde se brinden servicios de Internet de navegación y correo electrónico a personas naturales.
b) **Entorno Internet:** espacio de alcance mundial, creado mediante el empleo de las Tecnologías de la Información y la Comunicación y soportado por el sistema de recursos de Internet, protocolos de comunicación, lenguajes y herramientas de programación para Internet; que permiten el desarrollo y la operación de aplicaciones, servicios, productos y sistemas para utilizar la información, que se encuentre en diferentes plataformas y sistemas de bases de datos de manera interactiva e integrada; con fines informativos, divulgativos, educacionales, comerciales y de gestión institucional entre otros.

c) **Licencia de operación:** título habilitante mediante el cual se faculta a su tenedor para la operación de las áreas de Internet.
d) **Proveedor de servicios de acceso a Internet al Público:** persona jurídica o natural autorizada para prestar Servicios Públicos de Acceso a Internet a personas naturales en áreas de internet.
e) **Proveedor de Servicios Públicos de Acceso a Internet:** persona jurídica que recibe una autorización para prestar uno o varios tipos de servicios del Entorno Internet, en todo el territorio nacional.
f) **Servicios Públicos de Transmisión de Datos:** servicio final de telecomunicaciones por medio del cual se proporciona la capacidad completa para la comunicación de datos entre unidades funcionales, conforme a protocolos definidos. Este servicio contempla las modalidades local, nacional e internacional.
g) **Telecomunicaciones:** transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilos, radioelectricidad, medios ópticos u otros sistemas ópticos o electromagnéticos.
h) **Titular:** persona a la que se le otorga por el Ministerio de Comunicaciones la autorización para brindar servicios públicos de acceso a Internet en áreas de Internet.
i) **Transmisión de Datos**: acción de transportar informaciones, conforme a protocolos definidos, de un punto a otro o a varios puntos, con el uso de líneas físicas conductoras eléctricas, cables, fibras ópticas, satélites o enlaces inalámbricos para conducir señales; y equipos terminales para transmitirla y recibirla, con o sin almacenamiento intermedio.

Artículo 3. El presente Reglamento se aplica a aquella persona jurídica o natural acreditada como trabajador por cuenta propia de agente de telecomunicaciones, en lo adelante el Titular, que recibe una licencia de operación para prestar Servicios Públicos de Acceso a Internet en áreas de Internet a personas naturales.

Artículo 4. El proveedor soporta sus servicios sobre las Redes Públicas de Telecomunicaciones y en particular sobre la infraestructura y servicios de la Red Pública de Transmisión de Datos, hace uso de la plataforma autorizada donde se soportan los servicios que son ofrecidos por estos, la cual debe cumplir con los procesos de consulta a los organismos, en correspondencia con la legislación vigente y lo que establece el presente Reglamento.

Artículo 5. Los proveedores se clasifican, por su alcance geográfico en locales, municipales, provinciales, regionales y nacionales.

CAPÍTULO II
DE LA LICENCIA DE OPERACIÓN

Artículo 6. La condición de proveedor se otorga mediante aprobación y expedición de la Licencia de Operación, por la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones, en lo adelante UPTCER y la licencia corresponde a toda su extensión territorial.

Artículo 7. La solicitud debe contar con los documentos siguientes:

a) Carta de solicitud con información de los datos generales de la persona;
b) copia certificada del poder o resolución de designación del representante legal del titular; en caso de personas naturales, documento que acredite que es trabajador por cuenta propia como agente de telecomunicaciones y el contrato firmado con el operador público de telecomunicaciones;
c) documento con información acerca de aspectos técnicos del servicio, el equipamiento disponible para ello, cantidad de áreas de Internet y su localización; y
d) otros documentos de interés que se soliciten por la Dirección General de Informática, en lo adelante DGI, del Ministerio de Comunicaciones, en lo adelante MINCOM, como requisito adicional a lo regulado por el presente Reglamento.

Artículo 8. Los datos declarados pueden ser objeto de comprobación por los inspectores del MINCOM.

Artículo 9. Se exceptúan de solicitar autorización al MINCOM aquellos proveedores que hayan recibido la autorización para prestar Servicios Públicos de Acceso a Internet, y los que están autorizados por el MINCOM para brindar los servicios de acceso de Internet al público con anterioridad a la fecha de aprobación de este Reglamento; en todos los casos los proveedores tienen que actualizar la información de cada área de Internet previo a la activación de los servicios para su inscripción en el Control Administrativo Central Interno del MINCOM.

Artículo 10. La Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico (UPTCER), queda encargada de efectuar el análisis de la solicitud, el otorgamiento o denegación de la condición de proveedor, de la expedición, modificación o renovación de la licencia de operación de proveedor y de la inscripción de la información en el Control.

Artículo 11. La UPTCER expide la licencia de operación que permite al proveedor brindar los Servicios de Acceso a Internet al Público y disponen de hasta treinta (30) días hábiles para expedir la licencia a los solicitantes que reúnan los requisitos establecidos y sean aceptados o para notificar a los no aceptados.

Artículo 12. La Licencia de operación expedida tiene un plazo de vigencia de cinco (5) años. Cualquier modificación en los parámetros informados en el momento de la inscripción en el Control Administrativo Central Interno del MINCOM debe ser actualizado por el titular o su representante legal en la UPTCER. La licencia de operación para el caso de los proveedores de Servicios Públicos de Acceso a Internet se exceptúa de pago; no obstante, quedan obligados a mantener actualizado en la UPTCER, cualquier modificación en los parámetros informados en el momento de la inscripción.

Artículo 13. La Licencia de Operación expedida es un requisito indispensable para que l*os* proveedores presten sus servicios y debe ser renovada hasta sesenta (60) días antes del vencimiento del plazo de vigencia, mediante la presentación a la UPTCER, del documento de solicitud de renovación, vencido el plazo de vigencia, no puede brindar el servicio y el titular debe efectuar todos los trámites de renovación como una nueva solicitud.

Artículo 14. Los proveedores abonan por los derechos de licencia de operación de los servicios, la cantidad de trescientos pesos ($300.00 CUP), y ciento cincuenta pesos ($150.00 CUP) por renovación o modificación de esta; realizan el pago directamente en el Banco según establece la legislación vigente del Ministerio de Finanzas y Precios y presentan el comprobante de pago a la UPTCER para la obtención de la licencia, cuya copia se anexa al expediente.

Artículo 15. Los proveedores presentan la licencia de operación recibida al Proveedor de Servicios Públicos de Acceso a Internet para contratar los Servicios Públicos de Transmisión de Datos y el acceso a la plataforma autorizada.

Artículo 16. Los proveedores no pueden ceder o gravar en forma alguna, en todo o en parte, a favor de un tercero, los derechos que son objeto de esta licencia.

Artículo 17. Constituyen causas para retirar la licencia de operación por parte de la UPTCER las siguientes:

a) El vencimiento del plazo por el que fue otorgada la licencia de operación sin haberse solicitado, en su caso, su renovación.
b) La invalidez de la licencia de operación por los inspectores de la Oficina Territorial de Control del MINCOM, en lo adelante OTC, ante el incumplimiento, entre otras, de lo dispuesto en el presente Reglamento; en la legislación sobre telecomunicaciones en general y en específico las relacionadas con los Servicios de Internet y sobre la seguridad.
c) La renuncia a la licencia de operación por parte del proveedor.
d) La no prestación del servicio en el plazo que se establezca en la licencia de operación.
e) La extinción de la persona jurídica o el fallecimiento o declaración de emigrante de la persona natural, como proveedor.
f) La cesión o gravamen a favor de tercero, de los derechos que son objeto de la licencia de operación otorgada.
g) Las demás que correspondan, de conformidad con la legislación vigente.

CAPÍTULO III
DE LAS NORMAS TÉCNICAS, LA HOMOLOGACIÓN Y LOS ACUERDOS DE NIVEL DE SERVICIOS

Artículo 18. Las normas técnicas aplicables a la infraestructura sobre la que se soportan los servicios de este proveedor, son establecidas en el país según la legislación vigente, de acuerdo con las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT), o de otros organismos internacionales, de cuyos tratados Cuba sea Estado parte.

Artículo 19. Los equipos que se conecten a las redes públicas de telecomunicaciones o hagan uso del espectro radioeléctrico para la prestación del servicio deben estar Homologados, según lo establecido y cumplir las disposiciones vigentes para el empleo del espectro radioeléctrico en el país.

Artículo 20. Los proveedores establecen dentro de sus contratos de servicio con el operador de servicios públicos de telecomunicaciones, los indicadores de calidad que definan y garanticen los parámetros de la calidad del servicio, que cumplan con las recomendaciones internacionales, con las regulaciones nacionales vigentes y con aquellas que las partes acuerden complementariamente.

Artículo 21. Las partes acuerdan, según las regulaciones vigentes, entre otros indicadores y parámetros de calidad de servicio; los tipos de medición de los niveles de calidad que hacen de manera independiente, la periodicidad de la medición de cada indicador, las condiciones bajo las cuales existe intercambio de información sobre estos, los medios empleados para el intercambio de la información y los períodos dentro de los cuales se acepta por la otra parte la calificación que se haga de los mencionados niveles de servicio.

CAPÍTULO IV
DE LAS OBLIGACIONES EN CUANTO A LA ORGANIZACIÓN Y FUNCIONAMIENTO DE LOS PROVEEDORES

Artículo 22. Los proveedores se organizan y operan según las obligaciones siguientes:

a) Comenzar la operación de los servicios en cada área de Internet declarada en el plazo que fija la licencia de operación y cumplir con los términos legales, técnicos, económicos u operativos que esta establece;
b) poseer un Reglamento específico de organización y funcionamiento para prestar los servicios licenciados, el cual debe contener al menos los aspectos que den respuesta al cumplimiento de sus obligaciones organizativas, así como las obligaciones del proveedor y del cliente en la realización del servicio. El Reglamento debe ser elaborado en un plazo máximo de ciento ochenta (180) días, contados a partir de otorgada la licencia de operación;
c) garantizar la información necesaria y oportuna sobre la introducción de cambios tecnológicos a realizarse en los servicios;
d) mantener debidamente informados a los clientes sobre las características de los servicios en operación, las tarifas, las condiciones para su utilización y otra información que resulte de interés a estos;
e) acatar las disposiciones y requerimientos emitidos por los órganos de la Defensa, la Seguridad y el Orden Interior del país ante situaciones excepcionales;
f) permitir y facilitar la realización de las inspecciones de documentos, la infraestructura y los servicios en operación que incluyen el acceso a los equipos e instalaciones relacionadas con la licencia de operación otorgada, que se indiquen por la OTC, la Oficina de Seguridad para las Redes Informáticas, en lo adelante OSRI y demás autoridades competentes;
g) brindar las informaciones establecidas u otras que se les demanden por el MINCOM;
h) ofertar los servicios en correspondencia con las tarifas aprobadas según el marco jurídico vigente;
i) establecer un sistema eficiente de recepción y solución de quejas y de ejecución de reparaciones de fallas en los servicios proporcionados; y
j) garantizar la seguridad lógica y la física de los equipos en red.

Artículo 23. El proveedor de Servicio Público de Acceso a Internet que proporciona la plataforma autorizada para el servicio, adicionalmente a lo establecido en su reglamentación específica, cumple las obligaciones siguientes:

a) Establecer un sistema de recepción y solución de quejas y de ejecución de reparaciones de fallas en los servicios proporcionados;
b) implementar las medidas y herramientas que garanticen la seguridad de las infraestructuras de la red y la detección e investigación de incidentes de seguridad;
c) reportar los incidentes de seguridad informática que se detecten por las vías y procedimientos establecidos en la legislación vigente;
d) contar, para la operación de los servicios, con personal titulado y certificado, según corresponda, encargado de la administración, gestión y seguridad informática de estos, que garanticen el registro de los clientes del servicio;
e) establecer los procedimientos que aseguren la identificación del origen de los accesos, así como su registro y conservación por un tiempo no menor de un (1) año;
f) tramitar la aprobación requerida para la utilización de cualquier tipo de aplicación que implique el encriptamiento de la información a transmitir; y
g) adoptar las medidas necesarias para:

    1) impedir el acceso a sitios cuyos contenidos sean contrarios al interés social, la moral y las buenas costumbres; así como el uso de aplicaciones que afecten la integridad o la seguridad del Estado; y
    2) contrarrestar el envío de mensajes masivos dañinos a través de las redes de telecomunicaciones, que utilizan las Tecnologías de la Información y la Comunicación; así como el efecto dañino de los programas malignos.

Artículo 24. Los proveedores se mantienen informados del cumplimiento de las obligaciones del artículo precedente.

Artículo 25. La OTC controla y supervisa que el operador público de telecomunicaciones garantice la igualdad de condiciones y el trato no discriminatorio, en la provisión de los servicios públicos de infraestructura de red de telecomunicaciones a todos los proveedores de Servicios de Acceso a Internet al Público.

CAPÍTULO V
MEDIDAS Y PROCEDIMIENTOS A APLICAR ANTE INCUMPLIMIENTOS DEL PROVEEDOR

Artículo 26. El proveedor que incumpla lo dispuesto en el presente Reglamento y en las disposiciones legales vigentes en la materia, está sujeto a la aplicación de las medidas siguientes:

a) Notificación preventiva;
b) invalidación temporal o parcial o la cancelación, de las licencias de operación administrativamente concedidas por la UPTCER; y
c) suspensión temporal, parcial o la cancelación de los servicios que haya contratado con el proveedor de Servicios Públicos de Transmisión de Datos y Acceso a Internet debidamente

reconocido y autorizado por el MINCOM.

Artículo 27. El inspector de la OTC del MINCOM es la autoridad facultada para aplicar las medidas referidas en el artículo anterior e informar a la UPTCER sobre la medida impuesta y la decisión acerca de su aplicación.

Artículo 28. El proveedor sujeto a la aplicación de las medidas descritas anteriormente, puede reclamar en primera instancia ante al director de la OTC correspondiente, en el plazo de diez (10) días hábiles contados a partir de la fecha de notificación de la medida, formulan las alegaciones y ofrecen las pruebas que estimen convenientes a su derecho. A su vez el director de la OTC dispone de un plazo de treinta (30) días hábiles para dar respuesta a dicha apelación.

Artículo 29. El proveedor que desee impugnar la decisión de la primera instancia de reclamación, dispone de un plazo de diez (10) días hábiles a partir de la notificación de esta, para solicitar una revisión ante el director de la DGI, el cual dispone de un plazo de sesenta (60) días hábiles contados a partir del recibo oficial de la reclamación, para resolver lo que proceda sobre esta, contra esta decisión no cabe otro recurso por vía administrativa.

Artículo 30. El proveedor que haya sido objeto de una medida por incumplimiento, una vez resuelta la causa que dio lugar a la medida impuesta, puede presentar a la UPTCER su solicitud de licencia de operación, donde se toma en cuenta la información presentada y una vez comprobada por los inspectores de la OTC la solución de las deficiencias detectadas, se determina sobre el otorgamiento de la nueva licencia de operación.

SEGUNDO: El proveedor tiene que presentar su licencia de operación al operador público de telecomunicaciones, para solicitar, mantener o ampliar los servicios de conectividad.

TERCERO: El director general de la UPTCER queda responsabilizado con la elaboración de los procedimientos necesarios para el otorgamiento, renovación o modificación de las licencias de operación en un plazo de sesenta (60) días posteriores a su publicación en la Gaceta Oficial.

CUARTO: Los directores generales de Informática, de Comunicaciones y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, el director de Inspección y los directores territoriales de control del MINCOM, quedan encargados según corresponda, del control del cumplimiento de lo que por la presente se dispone.

DISPOSICIÓN TRANSITORIA

ÚNICA: Lo dispuesto en la presente Resolución no se aplica a las personas naturales hasta tanto se autorice este servicio como una actividad a realizarse como trabajo por cuenta propia.

DISPOSICIONES FINALES

PRIMERA: Se derogan las resoluciones del ministro de la Informática y las Comunicaciones No. 179, de fecha 7 de octubre de 2008 y No. 102, de fecha 16 de junio de 2011.

SEGUNDA: La presente resolución entra en vigor a los sesenta (60) días de su publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE a los directores generales de Informática, de Comunicaciones, de la Unidad Presupuestada de Control del Espectro Radioeléctrico y a los directores territoriales de control, pertenecientes al Ministerio de Comunicaciones, al presidente ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A. y a los Proveedores de Servicios de Acceso a Internet al Público.

COMUNÍQUESE a los viceministros, a los directores de Inspección y de Regulaciones, al director general de la Oficina de Seguridad para las Redes Informáticas, pertenecientes al Ministerio de Comunicaciones así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 29 días del mes de septiembre de 2017.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 254/2017

POR CUANTO: El Acuerdo No. 8151 del Consejo de Ministros, de fecha 22 de mayo de 2017, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de estos.

POR CUANTO: La Resolución No. 31 del ministro de la Informática y las Comunicaciones, de fecha 24 de enero del 2008, aprobó el Reglamento para los proveedores de servicio público de acceso a internet, el cual es preciso actualizar atendiendo a la experiencia acumulada y ajustándolo a las exigencias del desarrollo de las telecomunicaciones y las Tecnologías de la Información y la Comunicación en el país, por lo que es necesario emitir una nueva disposición normativa que derogue la referida anteriormente.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el inciso a), del Artículo 100 de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO PARA LOS PROVEEDORES DE SERVICIO PÚBLICO DE ACCESO A INTERNET

CAPÍTULO I
OBJETO, GENERALIDADES Y LEGISLACIÓN APLICABLE

Artículo 1. El objeto del presente Reglamento es el establecimiento de las normas para la organización, funcionamiento, aprobación y expedición de licencias de operación en el país del Proveedor de Servicios Públicos de Acceso a Internet, en lo adelante el proveedor.

Artículo 2. A los efectos del presente Reglamento, los términos que se citan a continuación tienen el significado siguiente:

a) **Coubicación:** es la localización en las instalaciones de un operador de los equipos de telecomunicaciones de otro operador o proveedor a los fines del acceso, la interconexión o la conexión. Esta localización puede incluir, en dependencia de las disponibilidades y el plan de desarrollo de cada operador público involucrado, la utilización del espacio físico y los servicios auxiliares, tales como energía eléctrica, seguridad, climatización, sistema de tierra y otros.

b) **Enlaces de telecomunicaciones públicos:** enlaces entre dos o más puntos, que permiten la transmisión de la información extremo a extremo, y se presta a través de la red pública de telecomunicaciones.

c) **Proveedor de servicios públicos de acceso a Internet:** persona jurídica que recibe una autorización para prestar uno o varios tipos de servicios del Entorno Internet, en todo el territorio nacional.

d) **Red privada de datos:** red de telecomunicaciones cuya infraestructura de red está instalada en una misma localidad o en distintas localidades geográficas e interconectadas entre sí por enlaces de telecomunicaciones públicos y propios, que satisface las necesidades de transmisión de datos de su titular.

e) **Red pública de telecomunicaciones:** red de telecomunicaciones que se explota principalmente para prestar servicios públicos de telecomunicaciones y Tecnologías de la Información y la Comunicación.

f) **Representante legal del Titular:** persona natural designada a los efectos de ostentar la representación del titular.

g) **Servicio Público de Acceso a Internet:** servicio público de telecomunicaciones que permite la interconexión mundial a redes de comunicación que utilizan la familia de protocolos TCP/IP.

h) **Servicio Público de Telecomunicaciones:** servicio destinado a satisfacer las necesidades de telecomunicaciones y de las Tecnologías de la Información y la Comunicación del público en general y se presta a través de redes expresamente autorizadas para ello.
i) **Titular:** persona jurídica a la que se le otorga la autorización por el Ministerio de Comunicaciones para brindar los Servicios Públicos de Acceso a Internet.
j) **Transmisión de Datos:** acción de transportar informaciones, conforme a protocolos definidos, de un punto a otro o a varios puntos, con el uso de líneas físicas conductoras eléctricas, cables, fibras ópticas, satélites o enlaces inalámbricos para conducir señales; y equipos terminales para transmitirla y recibirla, con o sin almacenamiento intermedio.

Artículo 3. El régimen jurídico básico por el que se rigen las prestaciones de estos servicios se determina por las concesiones administrativas y autorizaciones otorgadas para la prestación del servicio público de telecomunicaciones, por las disposiciones legales vigentes sobre el uso del espectro radioeléctrico, por el presente Reglamento y por la legislación de telecomunicaciones en general.

CAPÍTULO II
DE LA AUTORIZACIÓN

Artículo 4. La condición de proveedor se otorga mediante Resolución dictada por el ministro de Comunicaciones.

Artículo 5. El representante facultado por la entidad interesada en brindar Servicios Públicos de Acceso a Internet, presenta la solicitud de autorización a la dirección general de Informática del Ministerio de Comunicaciones, en lo adelante DGI.

Artículo 6. Los documentos básicos que se requieren para la solicitud de autorización son los siguientes:

a) Copia certificada del poder o resolución de designación del representante legal de la entidad;
b) proyecto de explotación de los servicios a brindar, plan de explotación, técnicas a utilizar, cobertura geográfica por territorios y a nivel nacional, modalidades de acceso, tarifas propuestas de los servicios; así como todo aquello que el solicitante estime conveniente para la óptima explotación de sus servicios;
c) presentar la documentación de conclusión del proceso de aprobación de la consulta a los organismos, según el Reglamento del Proceso Inversionista sobre la plataforma informática donde se soportan los servicios en caso de no ser de la autorizada; y
d) otros documentos de interés que se soliciten por la DGI como requisito adicional a lo regulado por el presente Reglamento.

Artículo 7. Los datos declarados pueden ser objeto de comprobación por los inspectores de las Oficinas Territoriales de Control del Ministerio de Comunicaciones, en lo adelante OTC.

Artículo 8. La DGI a partir de la recepción de la solicitud de autorización, analiza esta de conjunto con la dirección general de Comunicaciones, en lo adelante DGC y la dirección de Regulaciones del Ministerio de Comunicaciones, y ante la falta de información, la DGI solicita al interesado su

completamiento y confecciona el expediente en un plazo de hasta treinta (30) días hábiles para ser presentado a la aprobación del ministro. En caso de denegación emite carta al interesado que informa el rechazo y las razones de este.

Artículo 9. La DGI inscribe a los proveedores autorizados en el Control Administrativo Central Interno del Ministerio de Comunicaciones y una vez emitida la resolución ministerial se le entrega la licencia de operación al proveedor, la que tiene diez (10) años de vigencia.

Artículo 10. Las autorizaciones para la explotación de servicios públicos de acceso a Internet no son transferibles.

Artículo 11. La Licencia de Operación expedida es un requisito indispensable para que l*os* proveedores presten sus servicios y debe ser renovada hasta sesenta (60) días antes del vencimiento del plazo de vigencia, mediante la presentación a la DGI, del documento de solicitud de renovación. Una vez vencido el plazo, no puede brindar el servicio y el titular debe efectuar todos los trámites como una nueva solicitud.

Artículo 12. El proveedor comunica a la DGI cualquier modificación en la información presentada, a los efectos de su recepción, análisis e incorporación de esta al Control Administrativo Central Interno del Ministerio de Comunicaciones.

Artículo 13. El proveedor por los derechos de autorización abona trescientos pesos ($300.00 CUP) y por los trámites de renovación o de modificación ciento cincuenta pesos ($150.00 CUP). Este pago se hace directamente en el Banco según establece la legislación vigente del Ministerio de Finanzas y Precios y se presenta el comprobante de pago a la DGI para la obtención de la licencia, cuya copia se anexa al expediente.

Artículo 14. La autorización se retira por las causas siguientes:

a) La revocación de la autorización, cuando se produzcan incumplimientos de las condiciones o requisitos legales, técnicos, económicos, operativos o de seguridad establecidos; según lo dispuesto en la presente Resolución o sus disposiciones complementarias, así como por violaciones de las regulaciones vigentes sobre los servicios autorizados;
b) el vencimiento del plazo por el que fue otorgada la licencia sin haberse solicitado su renovación;
c) la renuncia solicitada por escrito y fundamentada por el representante legal del Titular, previa comunicación a la DGI, con noventa (90) días naturales de antelación a la fecha en que se pretenda que surta efectos la renuncia;
d) la disolución de la entidad autorizada; y
e) las demás que correspondan, de conformidad con la legislación vigente.

CAPÍTULO III
DE LAS OBLIGACIONES EN CUANTO A LA ORGANIZACIÓN Y FUNCIONAMIENTO DE LOS PROVEEDORES

Artículo 15. El proveedor está obligado a:

a) Utilizar los servicios portadores finales o de difusión existente de la red pública de telecomunicaciones, sin vulnerar las concesiones administrativas otorgadas a las empresas de telecomunicaciones debidamente reconocidas y autorizadas por el Estado cubano;
b) admitir como usuarios del servicio a las personas que lo deseen;
c) implementar las medidas y herramientas que garanticen la seguridad de la infraestructura de la red, los servicios que presta y la detección e investigación de incidentes de seguridad;
d) reportar los incidentes de seguridad informática que se detecten por las vías y procedimientos establecidos en la legislación vigente;
e) gestionar y controlar eficientemente el uso adecuado de las direcciones IP que le han sido asignadas;
f) cumplir los requisitos técnicos del servicio que le sirve de soporte, incluidos los puntos de conexión, así como lo estipulado en las condiciones de interconexión;
g) establecer de forma contractual su conexión al Punto de Intercambio de Tráfico, en lo adelante IXP (Internet Exchange Point en inglés);
h) acatar las disposiciones establecidas por los órganos de la Defensa, la Seguridad y el Orden Interior del país ante situaciones excepcionales;
i) cumplir con la calidad del servicio contratado con sus usuarios;
j) brindar a sus usuarios a través de su sitio Web, información sobre el uso y tráfico de los enlaces contratados;
k) informar debidamente de los puntos o nodos de acceso, tanto al Ministerio de Comunicaciones, como a los usuarios;
l) garantizar que los equipos que se conecten a las redes públicas de telecomunicaciones o hagan uso del espectro radioeléctrico para la prestación del servicio posean el correspondiente Certificado de Homologación expedido por la DGC;
m) elaborar un plan de contingencia para la mitigación de los riesgos que afecten el servicio;
n) permitir y facilitar la realización de las inspecciones de los equipos, edificios e instalaciones relacionadas con el servicio autorizado, por los inspectores de la OTC;
o) mantener debidamente informados a los usuarios de las características, facilidades, tarifas a aplicar y otras cuestiones relacionadas con el servicio ofertado; que se detallan en los correspondientes contratos a suscribir y advertir además con suficiente antelación de la modificación de las mismas;
p) mantener el principio de inviolabilidad y secreto de las comunicaciones, así como la confidencialidad de los aspectos requeridos, de conformidad con lo dispuesto en la Constitución de la República y la legislación vigente;
q) garantizar la protección y el tratamiento de los datos personales de sus clientes;
r) requerir la presentación de la licencia de operación a la red privada de datos que solicite sus servicios;

s) garantizar a sus usuarios de forma fácil la administración de los servicios contratados que lo requieran; y
t) brindar las informaciones establecidas u otras que se les demanden por el Ministerio de Comunicaciones.

CAPÍTULO IV
DE LAS NORMAS TÉCNICAS, LA HOMOLOGACIÓN Y LOS ACUERDOS DE NIVEL DE SERVICIOS

Artículo 16. Las normas técnicas aplicables a la infraestructura sobre la que se soportan los servicios del proveedor son establecidas en el país según la legislación vigente, de acuerdo con las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT), o de otros organismos internacionales, de cuyos tratados Cuba sea Estado parte.

Artículo 17. El proveedor está obligado a cumplir las especificaciones de los puntos de conexión de los servicios de soporte que utilicen. Las interfaces entre los puntos de interconexión y el proveedor del servicio deben estar normalizadas, procurándose siempre que sea posible, utilizar las más avanzadas técnicamente.

Artículo 18. Los parámetros de calidad de los Servicios Públicos de Acceso a Internet son regidos por los acuerdos de niveles de servicio en sus conexiones con el IXP con estos fines:

a) El proveedor está obligado a establecer de forma contractual con el operador público de telecomunicaciones los niveles de calidad de los servicios de manera que cumplan con las recomendaciones nacionales o internacionales que hayan sido acordadas. De no existir acuerdo entre las partes, se somete la discrepancia por escrito a la DGI, la cual tiene hasta treinta (30) días hábiles para su resolución. La misma de considerarlo pertinente, cita a las partes para escuchar sus argumentos; la decisión que se adopte es definitiva e inapelable.
b) Las partes acuerdan entre otros aspectos:

    1. Los tipos de mediciones de niveles de calidad que se hacen de manera independiente;
    2. la periodicidad de la medición de cada índice; y
    3. las condiciones bajo las cuales debe existir intercambio de información y los medios empleados para ello, así como los períodos dentro de los cuales se acepte por la otra parte la calificación que se haga de los niveles en cuestión.

c) El proveedor da a conocer a los clientes en sus respectivos contratos los acuerdos de los niveles de servicio e informa a la DGI según lo solicite.
d) Se recomienda coubicar siempre que sea posible, el equipamiento del proveedor en las instalaciones del Operador Público de Telecomunicaciones, tanto en el IXP como en centros técnicos de telecomunicaciones. En caso de no ser posible y a los efectos de facilitar la coubicación, el Operador Público de Telecomunicaciones debe adoptar las medidas pertinentes que viabilicen su realización, tanto desde el punto de vista técnico, como comercial, y debe

poner a disposición del proveedor, el espacio físico y todos los servicios auxiliares en sus propias instalaciones, en condiciones no discriminatorias.

e) Debe garantizarse al proveedor el libre acceso a los equipos instalados en la sede de la coubicación propiedad del Operador Público de Telecomunicaciones.

Artículo 19. Las partes pueden acordar, según las regulaciones vigentes y lo que complementariamente de mutuo acuerdo adopten, entre otros los aspectos siguientes:

a) Indicadores y parámetros de calidad de servicio;
b) tipos de medición de los niveles de calidad;
c) periodicidad de la medición de cada indicador;
d) condiciones bajo las cuales debe existir intercambio de información sobre los mismos;
e) medios empleados para el intercambio de la información; y
f) períodos dentro de los cuales se acepte por la otra parte la calificación que se haga de los mencionados niveles de servicio.

Artículo 20. Los equipos de telecomunicaciones y las Tecnologías de la Información y la Comunicación que los proveedores conecten a las redes públicas de telecomunicaciones o que hagan uso del espectro radioeléctrico tienen que haber obtenido previamente el correspondiente Certificado de Homologación según lo establecido en las normativas vigentes, el incumplimiento de ello, impide la obtención de servicios del Operador Público de Telecomunicaciones.

CAPÍTULO IV
DE LAS TARIFAS

Artículo 21. Los Servicios Públicos de Acceso a Internet se ofertan por sus proveedores con tarifas aprobadas según el marco jurídico vigente.

Artículo 22. Los pagos de coubicación son libremente negociados por las partes involucradas según los principios de neutralidad, transparencia y no discriminación, salvo los casos particulares de coubicaciones amparados por el marco jurídico vigente.

CAPÍTULO V
DE LOS INCUMPLIMIENTOS

Artículo 23. El proveedor que incumpla lo dispuesto en el presente Reglamento y en las disposiciones legales vigentes en la materia, está sujeto a la aplicación de las medidas siguientes:

a) Amonestación o advertencia, según el caso;
b) invalidación temporal o cancelación de la autorización concedida al titular; y
c) la aplicación de otras medidas que correspondan, de conformidad con el marco jurídico establecido en el país.

Artículo 24. Los inspectores de la OTC que detecten el incumplimiento de lo establecido por el presente Reglamento, notifican al proveedor y se envía copia de esta al director de la DGI, que informa al que resuelve para la imposición de las medidas.

Artículo 25. El proveedor sujeto a la aplicación de las medidas, puede apelar directamente o por medio de su representante legal, ante el que suscribe, en el plazo de diez (10) días hábiles contados a partir de la fecha de aplicada la medida, para lo cual formula las alegaciones y presenta las pruebas que crea convenientes a su derecho. El que suscribe dispone de sesenta (60) días hábiles para dar respuesta a dicha reclamación, contra esta decisión no cabe otro recurso por vía administrativa.

Artículo 26. El proveedor que haya sido objeto de una sanción que origine la cancelación de su licencia, puede una vez resuelta las causas que dieron lugar a la sanción impuesta y cumplido el tiempo de invalidación, presentar su solicitud de autorización a la DGI por medio de su representante legal. La DGI tiene en cuenta la información entregada, la cual es comprobada por los inspectores de la OTC verificando la solución de las deficiencias detectadas, para que la DGI presente al que suscribe las consideraciones sobre la solicitud de autorización.

SEGUNDO: El director general de Informática queda responsabilizado con la elaboración de los procedimientos necesarios para la implementación de lo dispuesto en la presente en un plazo de sesenta (60) días posteriores a su publicación en la Gaceta Oficial de la República de Cuba.

TERCERO: El director general de Informática, el director de Inspección y los directores territoriales de control del Ministerio de Comunicaciones, quedan encargados según corresponda, del control del cumplimiento de lo que por la presente se dispone.

DISPOSICIONES FINALES

PRIMERA: Derogar la Resolución No. 31, de fecha 24 de enero de 2008 y cuantas disposiciones legales de igual o inferior jerarquía se opongan a lo dispuesto en la presente Resolución.

SEGUNDA: La presente Resolución entra en vigor a los sesenta (60) días posteriores a su fecha de publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE al presidente ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A., al director general de Informática y a los directores de Inspección y territoriales de control pertenecientes al Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, de la Oficina de Seguridad para las Redes Informáticas y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y a los directores de Inspección y de Regulaciones, pertenecientes al Ministerio de Comunicaciones.

ARCHÍVESE el original en la dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 29 días del mes de septiembre del 2017.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 219/2016

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, radiocomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos.

POR CUANTO: La Resolución No. 179 "Reglamento para los proveedores de servicios de acceso a internet al público", de fecha 7 de octubre de 2008, tal como quedó modificada por la Resolución No.102, de fecha 16 de junio de 2011, ambas del Ministro de la Informática y las Comunicaciones, establece en sus artículos 6 y 9 el procedimiento de autorización a las entidades que desean brindar servicios de acceso de internet al público.

POR CUANTO: La Unión de Jóvenes Comunistas ha solicitado autorización al Ministro de Comunicaciones para que el Hotel Altahabana perteneciente a dicha organización, pueda brindar servicios de Acceso a Internet al Público; por lo que se ha considerado acceder a su solicitud, al valorar sus características y los servicios que están interesados en prestar a personas naturales; así como las condiciones creadas para brindarlos.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el Artículo 100 inciso a) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Autorizar a la Unión de Jóvenes Comunistas para que a través del Hotel Altahabana perteneciente a dicha organización, opere como Proveedor de Servicios de Acceso a Internet al Público, los que prestan a personas naturales a través de áreas de Internet acondicionadas para ello, las cuales se inscriben previamente en este Ministerio.

SEGUNDO: El Hotel Altahabana brinda los servicios de Acceso a Internet al Público, a través de la plataforma tecnológica "NAUTA" de la Empresa de Telecomunicaciones de Cuba, S.A. y cumple con lo regulado en el Reglamento de los proveedores de servicios de acceso a Internet al Público.

NOTIFÍQUESE a la primera secretaria del Comité Nacional de la Unión de Jóvenes Comunistas, al director del Hotel Altahabana y al presidente ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, Informática y de la Oficina de Seguridad para las Redes Informáticas, a los directores de Regulaciones, Inspección y de las oficinas territoriales de control, todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los 17 días del mes de octubre de 2016.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 73/2016

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de 28 de febrero de 2013, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, radiocomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos.

POR CUANTO: La Resolución No. 179 “Reglamento para los proveedores de servicios de acceso a internet al público”, de fecha 7 de octubre de 2008, tal como quedó modificada por la Resolución No.102, ambas del Ministro de la Informática y las Comunicaciones, de fecha 16 de junio de 2011, establece en sus artículos 6 y 9 el procedimiento de autorización a las entidades que desean brindar servicios de acceso de internet al público.

POR CUANTO: La entidad Cadena de Tiendas TRD Caribe, ha solicitado autorización al Ministro de Comunicaciones para brindar servicios de Acceso a Internet al Público, por lo que se ha considerado acceder a dicha solicitud, al valorar las características de la mencionada entidad y los servicios que están interesados en prestar a personas naturales; así como las condiciones creadas para brindar estos.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el inciso a), del Artículo 100 de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Autorizar a la entidad Cadena de Tiendas TRD Caribe a operar como Proveedor de Servicios de Acceso a Internet al Público, los que prestan a personas naturales a través de áreas de Internet acondicionadas para ello, las cuales se inscriben previamente en este Ministerio.

SEGUNDO: La entidad Cadena de Tiendas TRD Caribe brinda los servicios de Acceso a Internet al Público, a través de la plataforma tecnológica "NAUTA" de la Empresa de Telecomunicaciones de Cuba, S.A. y cumple con lo regulado en el Reglamento de los proveedores de servicios de acceso a Internet al Público.

NOTÍFÍQUESE a la Directora General TRD Caribe y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, Informática y de la Oficina de Seguridad para las Redes Informáticas, a los directores de Regulaciones, Inspección y de las oficinas territoriales de control de la Habana, todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los 15 días del mes de marzo de 2016.

Maimir Mesa Ramos

RESOLUCIÓN No. 325/2015

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, radiocomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos.

POR CUANTO: La Resolución No. 179 "Reglamento para los proveedores de servicios de acceso a internet al público" de fecha 7 de octubre de 2008, del Ministro de la Informática y las Comunicaciones, tal como quedó modificada por la Resolución No. 102 del Ministro de la Informática y las Comunicaciones, de fecha 16 de junio de 2011, establece en sus artículos 6 y 9 el procedimiento de autorización a las entidades que desean brindar servicios de acceso de internet al público y el tratamiento a seguir para su correspondiente inscripción.

POR CUANTO: La Empresa de Aplicaciones Informáticas *(*DESOFT) perteneciente al Grupo Empresarial de la Informática y las Comunicaciones (GEIC) ha solicitado autorización al Ministerio de Comunicaciones para brindar servicios de acceso a internet al público, por lo que se ha considerado acceder a dicha solicitud, al valorar las características de la mencionada entidad y los servicios que están interesados en prestar a personas naturales, así como las condiciones creadas para brindar éstos.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el inciso a), del Artículo 100 de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Autorizar a la Empresa de Aplicaciones Informáticas (DESOFT) perteneciente al Grupo Empresarial de la Informática y las Comunicaciones (GEIC) como Proveedor de Servicios de Acceso a Internet al Público, los que prestan a personas naturales a través de áreas de Internet acondicionadas para ello, las cuales se registran en este Ministerio.

SEGUNDO: La Empresa de Aplicaciones Informáticas (DESOFT) brinda los servicios de Acceso a Internet al Público, a través de la plataforma tecnológica "NAUTA" de la Empresa de Telecomunicaciones de Cuba, S.A. y debe cumplir con lo regulado en el Reglamento de los proveedores de servicios de acceso a Internet al Público.

NOTIFÍQUESE al director de la Empresa de Aplicaciones Informáticas (DESOFT) y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, Informática y de la Oficina de Seguridad para las Redes Informáticas, al presidente del Grupo Empresarial de la Informática y las Comunicaciones, así como a los directores de Regulaciones, Inspección y territoriales de control, todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 29 días del mes de diciembre de 2015.

Maimir Mesa Ramos

RESOLUCIÓN No. 296/2015

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en su numeral Cuarto, apartado Primero, dispone que el ministerio de Comunicaciones tiene como función

específica, la de ordenar, regular y controlar los servicios de telecomunicaciones e informáticos, nacionales e internacionales y la implementación de los mismos.

POR CUANTO: La Corporación CIMEX S.A., ha solicitado autorización al ministerio de Comunicaciones para brindar servicios de acceso a internet al público, en virtud de lo establecido por éste ministerio; por lo que se ha tomado en consideración las características de la mencionada entidad y los servicios que están interesados en prestar por medio de áreas de Internet a personas naturales así como las condiciones creadas para brindar estos.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el inciso a), del Artículo 100 de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Autorizar a la Corporación CIMEX S.A. a operar como proveedor de servicios de acceso a internet al público, los que prestan a personas naturales a través de áreas de internet acondicionadas para ello, las cuales se inscriben previamente en este Ministerio.

SEGUNDO: La Corporación CIMEX S.A. brinda los servicios de acceso a internet al público, a través de la plataforma tecnológica ¨NAUTA¨ de la Empresa de Telecomunicaciones de Cuba, S.A., y cumple con lo regulado en el Reglamento de los proveedores de servicios de acceso a Internet al Público.

TERCERO: Las Oficinas Territoriales de Control del ministerio de Comunicaciones, quedan encargadas del cumplimiento de lo que por la presente se dispone.

NOTÍFÍQUESE al Presidente de la Corporación CIMEX S.A. y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A.

COMUNÍQUESE a los viceministros, al director de Regulaciones, a los directores generales de Comunicaciones, Informática y de la Oficina de Seguridad para las Redes Informáticas, pertenecientes todos al ministerio de Comunicaciones.

ARCHÍVESE el original en la dirección Jurídica del ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 30 días del mes de noviembre de 2015.

Maimir Mesa Ramos

RESOLUCIÓN No. 278/2015

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en su numeral Cuarto, apartado Primero, dispone que el ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, radiocomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos.

POR CUANTO: La Resolución No. 179, del ministro de la Informática y las Comunicaciones, de fecha 7 de octubre del 2008, en su Capítulo III, Sección Primera, Artículo 6, establece el procedimiento de autorización a las entidades que desean brindar servicios de Acceso a Internet al Público.

POR CUANTO: La Comercializadora de Servicios Médicos Cubanos, perteneciente al ministerio de Salud Pública, ha solicitado autorización al ministerio de Comunicaciones para brindar servicios de Acceso a Internet al Público, por lo que se ha considerado acceder a dicha solicitud, al valorar las características de la mencionada entidad y los servicios que están interesados en prestar a personas naturales, así como las condiciones creadas para brindar estos.

POR TANTO: En el ejercicio de las atribuciones conferidas en el Artículo 100 inciso a), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Autorizar a la Comercializadora de Servicios Médicos Cubanos a operar como Proveedor de Servicios de Acceso a Internet al Público, los que prestan a personas naturales a través de áreas de Internet acondicionadas para ello, las cuales se inscriben previamente en este ministerio.

SEGUNDO: La Comercializadora de Servicios Médicos Cubanos brinda los servicios de Acceso a Internet al Público, a través de la plataforma tecnológica “NAUTA” de la Empresa de Telecomunicaciones de Cuba, S.A., y cumple con lo regulado en el Reglamento de los proveedores de servicios de acceso a Internet al Público.

DESE CUENTA al ministro de Salud Pública.

NOTIFÍQUESE al Director de la Comercializadora de Servicios Médicos Cubanos y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A.

COMUNÍQUESE a los viceministros, directores generales y ministeriales, directores de Regulaciones e Inspección, directores territoriales de control y director general de la Oficina de Seguridad para las Redes Informáticas, y a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la dirección Jurídica del ministerio Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los 23 días del mes de octubre de 2015.

Maimir Mesa Ramos

RESOLUCIÓN No. 133/2015

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de 28 de febrero de 2013, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, radiocomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos.

POR CUANTO: La Resolución No. 179 del Ministerio de Comunicaciones, de fecha 7 de octubre del 2008, en su Capítulo III, Sección Primera, Artículo 6, establece el procedimiento de autorización a las entidades que desean brindar servicios de Acceso a Internet al Público.

POR CUANTO: La Agrupación Artística Gallega, asociación sin fines de lucro, ha solicitado autorización al Ministerio de Comunicaciones para brindar servicios de Acceso a Internet al Público, por lo que se ha considerado acceder a dicha solicitud, valorando las características de la mencionada entidad y los servicios que están interesados en prestar a personas naturales; así como las condiciones creadas para brindar estos.

POR TANTO: En el ejercicio de las atribuciones conferidas, en el Artículo 100 inciso a), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Autorizar a la Agrupación Artística Gallega a operar como Proveedor de Servicios de Acceso a Internet al Público, los que prestan a personas naturales a través de áreas de Internet acondicionadas para ello, las cuales tienen que ser registradas en este Ministerio.

SEGUNDO: La Agrupación Artística Gallega brinda los servicios de Acceso a Internet al Público, a través de la plataforma tecnológica “NAUTA” autorizada de la Empresa de Telecomunicaciones de Cuba, S.A., cumpliendo con lo regulado en el Reglamento de los proveedores de servicios de acceso a Internet al Público.

NOTÍFÍQUESE al Presidente de la Agrupación Artística Gallega y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A., ETECSA.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, Informática y de la Oficina de Seguridad para las Redes Informáticas, a los directores de Regulaciones, Inspección y Oficina Territorial de Control de La Habana, pertenecientes todos al Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 10 días del mes de junio de 2015.

Maimir Mesa Ramos

RESOLUCIÓN No. 534/2014

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, radiocomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos.

POR CUANTO: Teniendo en cuenta las características de Joven Club de Computación y Electrónica perteneciente al Ministerio de Comunicaciones y los servicios que este presta a la población a nivel nacional, en materia de informatización, así como las condiciones administrativas y técnicas creadas, las cuales le ha permitido brindar con eficiencia y seguridad los diferentes servicios que ofrece en la actualidad, hemos considerado conveniente emitir la presente Resolución que autorice a Joven Club de Computación y Electrónica a ejercer como proveedor de los servicios de acceso a Internet al público.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 100 inciso a), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Autorizar a la entidad Joven Club de Computación y Electrónica para operar como Proveedor de Servicios de Acceso a Internet al Público y prestar esos servicios a personas naturales a través de sus áreas de Internet.

SEGUNDO: Los Joven Club de Computación y Electrónica brindan los servicios autorizados a través de la plataforma tecnológica “NAUTA” de la Empresa de Telecomunicaciones de Cuba .S.A. y cumplen lo establecido en el Reglamento de proveedores de servicios de acceso a Internet al público.

NOTIFIQUESE al Director General de Joven Club de Computación y Electrónica y al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A.

COMUNIQUESE a los viceministros, directores generales de Comunicaciones e Informática y de la Oficina de Seguridad para las Redes Informáticas y al Director de Regulaciones, todos pertenecientes al Ministerio de Comunicaciones.

ARCHIVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLIQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los 25 días del mes de septiembre de 2014.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 248/2013

POR CUANTO: La Resolución No. 179 del Ministro de Comunicaciones, de fecha 7 de octubre de 2008, “Reglamento para los Proveedores de Servicios de Acceso a Internet al Público”, tal y como quedó modificada por la Resolución No. 102 de fecha 16 de junio de 2011 del propio ministro, establece las normas sobre la organización, funcionamiento y obligaciones de los proveedores para ser autorizados a prestar estos servicios, así como los procedimientos para el registro y expedición de las correspondientes licencias.

POR CUANTO: La Oficina del Historiador de la ciudad de la Habana, el Instituto de Información Científica Tecnológica, perteneciente al Ministerio de Ciencia, Tecnología y Medio Ambiente (IDICT) y la Empresa Cubana de Aeropuertos y Servicios Aeroportuarios (ECASA), perteneciente al Ministerio del Transporte han solicitado autorización al Ministerio de Comunicaciones para brindar servicios de Acceso a Internet al Público, en virtud de lo establecido por éste Ministerio; por lo que se ha tomado en consideración las características de las mencionadas entidades y los servicios que prestan por medio de sus Áreas de Internet a personas naturales; así como las condiciones creadas para brindar estos..

POR TANTO: En el ejercicio de la facultad que me está conferida por el numeral Cuarto, Apartado Tercero del Acuerdo No. 2817 de fecha 25 de noviembre de 1994 del Comité Ejecutivo del Consejo de Ministros;

RESUELVO:

PRIMERO: Autorizar a la Oficina del Historiador de la ciudad de La Habana, al Instituto de Información Científica Tecnológica (IDICT), perteneciente al Ministerio de Ciencia, Tecnología y Medio Ambiente y a la Empresa Cubana de Aeropuertos y Servicios Aeroportuarios (ECASA), perteneciente al Ministerio del Transporte, a operar como Proveedores de Servicios de Acceso a Internet al Público, los que prestarán esos servicios a personas naturales a través de sus áreas de Internet.

SEGUNDO: Las entidades antes referidas brindarán los servicios a través de la plataforma autorizada a la Empresa de Telecomunicaciones de Cuba S.A., ETECSA, cumpliendo con lo establecido en el referido "Reglamento de Proveedores de Servicios de Acceso a Internet al Público" y sus sucesivas modificaciones.

DÉSE CUENTA al Ministro de Ciencia, Tecnología y Medio Ambiente y al Ministro del Transporte.

NOTÍFÍQUESE al Historiador de la ciudad de La Habana; al Director del Instituto de Información Científica Tecnológica, perteneciente al Ministerio de Ciencia, Tecnología y Medio Ambiente; al Director de la Empresa Cubana de Aeropuertos y Servicios Aeroportuarios, perteneciente al Ministerio del Transporte y a la Presidente Ejecutiva de la Empresa de Telecomunicaciones de Cuba S.A., ETECSA.

COMUNÍQUESE a los viceministros, al Director de Regulaciones y Normas, a los directores generales de la Oficina de Seguridad para las Redes Informáticas y de la Agencia de Control y Supervisión del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 15 días del mes de julio de 2013.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 247/2013

POR CUANTO: La Resolución No. 179 del Ministro de Comunicaciones, de fecha 7 de octubre de 2008, "Reglamento para los Proveedores de Servicios de Acceso a Internet al Público", tal y como quedó modificada por la Resolución No. 102 de fecha 16 de junio de 2011 del propio ministro, establece las normas sobre la organización, funcionamiento y obligaciones de los proveedores para ser autorizados a prestar estos servicios, así como los procedimientos para el registro y expedición de las

correspondientes licencias.

POR CUANTO: La Corporación CIMEX S.A. ha solicitado autorización al Ministerio de Comunicaciones para que Residencial Tarará S.A., sociedad mercantil que integra su organización empresarial, brinde servicios de acceso a internet al público; en virtud de lo establecido por este Ministerio; por lo que se ha tomado en consideración las características de la mencionada entidad y los servicios que presta por medio de sus Áreas de Internet a personas naturales; así como las condiciones creadas para brindar estos.

POR TANTO: En el ejercicio de la facultad que me está conferida por el numeral Cuarto, Apartado Tercero del Acuerdo No. 2817 de fecha 25 de noviembre de 1994 del Comité Ejecutivo del Consejo de Ministros;

RESUELVO:

PRIMERO: Autorizar a Residencial Tarará S.A., integrante de la Corporación CIMEX S.A., a operar como proveedor de servicios de acceso a internet al público, que serán prestados a personas naturales a través de sus áreas de internet.

SEGUNDO: Residencial Tarará S.A. brindará los servicios a través de la plataforma autorizada a la Empresa de Telecomunicaciones de Cuba S.A., ETECSA, cumpliendo con lo establecido en el referido “Reglamento para los Proveedores de Servicios de Acceso a Internet al Público” y sus sucesivas modificaciones.

NOTÍFÍQUESE al Presidente de la Corporación CIMEX, S.A. y a la Presidente Ejecutiva de la Empresa de Telecomunicaciones de Cuba S.A., ETECSA.

COMUNÍQUESE a los viceministros, al Director de Regulaciones y Normas, a los directores generales de la Oficina de Seguridad para las Redes Informáticas y de la Agencia de Control y Supervisión del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 15 días del mes de julio de 2013.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 246/2013

POR CUANTO: La Resolución No. 179 del Ministro de Comunicaciones, de fecha 7 de octubre de 2008, "Reglamento para los Proveedores de Servicios de Acceso a Internet al Público", tal y como quedó modificada por la Resolución No. 102 de fecha 16 de junio de 2011 del propio ministro, establece las normas sobre la organización, funcionamiento y obligaciones de los proveedores para ser autorizados a prestar estos servicios, así como los procedimientos para el registro y expedición de las correspondientes licencias.

POR CUANTO: La Dirección General del Grupo Empresarial Campismo Popular adscripto al Ministerio del Turismo, ha solicitado autorización al Ministerio de Comunicaciones para que las villas internacionales Aguas Claras y Laguna Grande ubicadas en la provincia de Pinar del Río, así como Guajimico en la provincia de Cienfuegos y el Hotel Rancho del Tesoro del Municipio Especial Isla de la Juventud, pertenecientes a su organización, brinden servicios de acceso a Internet al público, en virtud de lo establecido por este Ministerio; por lo que se ha tomado en consideración las características de la mencionada entidad y los servicios que presta por medio de sus Áreas de Internet a personas naturales; así como las condiciones creadas para brindar estos.

POR TANTO: En el ejercicio de la facultad que me está conferida por el numeral Cuarto, Apartado Tercero del Acuerdo No. 2817 de fecha 25 de noviembre de 1994 del Comité Ejecutivo del Consejo de Ministros;

RESUELVO:

PRIMERO: Autorizar como Proveedores de Servicios de Acceso a Internet al Público a las entidades del Grupo Empresarial Campismo Popular, adscripto al Ministerio del Turismo, que se relacionan a continuación; las cuales prestarán sus servicios a personas naturales a través de sus áreas de Internet.

1. Villa Internacional Aguas Claras, provincia Pinar del Río.
2. Villa Internacional Laguna Grande, provincia Pinar del Río.
3. Villa Internacional Guajimico, provincia Cienfuegos.
4. Villa Internacional Hotel Rancho del Tesoro, municipio Especial Isla de la Juventud.

SEGUNDO: Las villas internacionales relacionadas en el apartado anterior brindan los servicios a través de la plataforma autorizada a la Empresa de Telecomunicaciones de Cuba S.A., ETECSA, cumpliendo con lo establecido en el referido "Reglamento de Proveedores de Servicios de Acceso a Internet al Público" y sus sucesivas modificaciones.

DÉSE CUENTA al Ministro del Turismo.

NOTÍFÍQUESE al Director General del Grupo Empresarial Campismo Popular y a la Presidente Ejecutiva de la Empresa de Telecomunicaciones de Cuba S.A., ETECSA.

COMUNÍQUESE a los viceministros, al Director de Regulaciones y Normas, a los directores

generales de la Oficina de Seguridad para las Redes Informáticas y de la Agencia de Control y Supervisión del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 15 días del mes de julio de 2013.

Maimir Mesa Ramos

Ministro

RESOLUCIÓN No. 6/2013

POR CUANTO: El Acuerdo No. 3736 del Comité Ejecutivo del Consejo de Ministros, de fecha 18 de julio del 2000, en su numeral Séptimo, apartado Segundo, dispone que el Ministerio de la Informática y las Comunicaciones es el organismo encargado de establecer, regular y controlar las normas técnicas y operacionales de todas las redes informáticas y sistemas de comunicaciones en general, nacionales e internacionales que funcionan en el país; además el numeral Noveno del propio apartado establece que está encargado de evaluar, proponer y otorgar la expedición y revocación de autorizaciones, permisos y licencias a operadores y proveedores de servicios informáticos, de telecomunicaciones y postales, privados o públicos, velando por su cumplimiento en el marco de su autoridad.

POR CUANTO: Mediante la Resolución No. 43 del Ministro de la Informática y las Comunicaciones, de fecha 3 de marzo de 2009, se autorizó a la Empresa de Tecnologías de la Información y Servicios Telemáticos Avanzados, CITMATEL, perteneciente al Ministerio de Ciencia, Tecnología y Medio Ambiente, como Proveedor de Servicios Públicos de Valor Agregado de Telecomunicaciones de Datos, entre ellos como Proveedor de Acceso a Internet, y mediante las resoluciones No. 159, de fecha 15 de octubre de 2007, No. 142, de 18 de junio de 2008 y la No. 120, de 29 de julio de 2009, todas del Ministro de la Informática y las Comunicaciones, se aprobaron las tarifas para los diferentes servicios que brinda CITMATEL.

POR CUANTO: Con el objetivo de hacer más efectiva la oferta de los servicios públicos de acceso a Internet además de lograr un mayor aprovechamiento de la sinergia y los recursos existentes, resulta conveniente revocar la autorización otorgada y disponer que los servicios que venía brindando dicha empresa, sean asimilados por la Empresa de Telecomunicaciones de Cuba, S.A., proveedor de estos servicios en el país, y derogar por consiguiente las resoluciones referidas.

POR TANTO: En el ejercicio de la facultad conferida por el numeral Cuarto, apartado Tercero del

Acuerdo No. 2817 del Comité Ejecutivo del Consejo de Ministros, de fecha 25 de noviembre de 1994;

RESUELVO:

PRIMERO: Revocar la autorización otorgada a la Empresa de Tecnologías de la Información y Servicios Telemáticos Avanzados, CITMATEL, perteneciente al Ministerio de Ciencia, Tecnología y Medio Ambiente, como Proveedor de Servicios Públicos de Valor Agregado de Telecomunicaciones de Datos, entre ellos como Proveedor de Acceso a Internet.

SEGUNDO: Traspasar a la Empresa de Telecomunicaciones de Cuba S.A., en lo adelante ETECSA, los servicios a terceros, que con carácter de Proveedor de Servicios Públicos de Valor Agregado de Telecomunicaciones de Datos, entre ellos como Proveedor de Acceso a Internet, venía ejecutando CITMATEL en el territorio nacional a los usuarios no comprendidos en el sistema del Ministerio de Ciencia, Tecnología y Medio Ambiente. El traspaso de estos servicios debe efectuarse sin afectaciones a los usuarios.

TERCERO: El que suscribe encargará a un Viceministro el control de la ejecución del traspaso a ETECSA, de los servicios a terceros antes mencionados que venía ejecutando ClTMATEL, al que se faculta además para emitir las indicaciones que sean pertinentes para el cumplimiento de lo que por la presente se dispone.

CUARTO: CITMATEL informará a sus usuarios acerca de la cesión de sus obligaciones a ETECSA, dentro de los treinta (30) días posteriores a la entrada en vigor de la presente Resolución, según lo establecido en el inciso n) del Artículo 12, del Reglamento para los Proveedores de Servicio Público de Acceso a Internet, aprobado por la Resolución No. 31, del Ministro de la Informática y las Comunicaciones, de fecha 24 de enero de 2008.

QUINTO: ETECSA aplicará las tarifas vigentes para la prestación de sus servicios a los usuarios de CITMATEL, lo que comunicará en el término de noventa (90) días antes de comenzar a prestar dichos servicios.

SEXTO: ETECSA y los usuarios de CITMATEL disponen de hasta noventa (90) días a partir de 1 de marzo de 2013, para la concertación de los nuevos contratos, antes de comenzar la prestación de los servicios.

SÉPTIMO: ETECSA a partir del día en que inicie la prestación de los servicios a los usuarios de CITMATEL, comienza a facturar, según las tarifas vigentes, los servicios que presta a CITMATEL como red privada del Ministerio de Ciencia, Tecnología y Medio Ambiente, debiendo esta cumplimentar el marco regulatorio vigente para las redes privadas de datos.

OCTAVO: El traspaso de los usuarios de CITMATEL comenzará a efectuarse a partir de 1 de marzo de 2013.

NOVENO: Derogar las resoluciones No. 159, No. 142, No. 120 y No. 43 de fechas 15 de octubre de 2007, 18 de junio de 2008, 29 de julio de 2009 y 3 de marzo de 2009, respectivamente.

DÉSE CUENTA al Ministro de Ciencia, Tecnología y Medio Ambiente y por su conducto a la Directora de la Empresa de Tecnologías de la Información y Servicios Telemáticos Avanzados, CITMATEL.

NOTIFÍQUESE a la Presidente Ejecutiva de la Empresa de Telecomunicaciones de Cuba, S.A.

COMUNÍQUESE a los Viceministros, al Director de la Dirección de Regulaciones y Normas, al Director General de la Agencia de Control y Supervisión y a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 15 días del mes de enero de 2013.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 24/2010

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000 cambió la denominación del Ministerio de Comunicaciones por la de Ministerio de la Informática y las Comunicaciones, para desarrollar las tareas y funciones que hasta el momento realizaba el Ministerio de Comunicaciones, así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sidero Mecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 30 de agosto del 2006, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: El Acuerdo No. 2817 de fecha 25 de noviembre de 1994, del Comité Ejecutivo del Consejo de Ministros, faculta a los Jefes de los Organismos de la Administración Central del Estado; a dictar en el límite de sus facultades y competencia, reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del Organismo; y en su caso, para los demás organismos, los órganos locales del poder popular, las entidades estatales, el sector cooperativo, mixto, privado y la población.

POR CUANTO: El Acuerdo No. 3736, de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo del Consejo de Ministros, establece que el Ministerio de la Informática y las Comunicaciones, es el organismo encargado de ordenar, regular y controlar los servicios informáticos y de telecomunicaciones, nacionales e internacionales y otros servicios afines en los límites del territorio nacional, así como, de conjunto con las organizaciones correspondientes, el Acceso a las Redes de Infocomunicaciones con Alcance Global. Además es la Autoridad encargada de evaluar, proponer y otorgar la expedición y revocación de concesiones, autorizaciones, permisos y licencias a operadores y proveedores de servicios informáticos y de telecomunicaciones, privados o públicos, velando por su cumplimiento en el marco de su autoridad.

POR CUANTO: La Resolución Ministerial No. 179 de fecha 7 de octubre del 2008, establece las normas para la organización, funcionamiento y obligaciones del Proveedor de Servicios de Acceso a Internet al Público.

POR CUANTO: El Ministerio del Turismo ha solicitado autorización para la prestación de Servicios de Acceso a Internet al Público, para un conjunto de entidades de ese sector, conforme a lo establecido en la referida norma del Por Cuanto precedente.

POR CUANTO: Para la autorización de este servicio, se ha tenido en cuenta las características de las entidades del Ministerio del Turismo y los servicios que prestan a personas naturales, así como las condiciones creadas en las mismas, para brindar Servicios de Acceso a Internet al Público.

POR TANTO: En el ejercicio de las facultades que me están conferidas

RESUELVO:

PRIMERO: Autorizar como Proveedores de Servicios de Acceso a Internet al Público a las entidades, del Ministerio del Turismo, que se relacionan a continuación; las cuales prestarán sus servicios a personas naturales en el territorio nacional a través de sus áreas de Internet.

1) Corporación de Turismo y Comercio Internacional Cubanacán S.A.
2) Grupo Empresarial Hotelero Gran Caribe S.A.
3) Grupo Empresarial Hotelero Islazul S.A.
4) Grupo Empresarial Extrahotelero Palmares S.A.
5) Unidad Presupuestada Oficina del Turismo, Ciudad Habana.
6) Complejo Las Terrazas S.A.
7) Grupo Empresarial Marinas y Náuticas Martín S.A.

SEGUNDO: Las entidades relacionadas en el Apartado anterior deben brindar los servicios autorizados, cumplimentando lo establecido en la Resolución No.179 de fecha 7 de octubre del 2008, del Ministerio de la Informática y las Comunicaciones.

TERCERO: La Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, queda encargada de controlar el cumplimiento de lo que por la presente se establece.

DESE CUENTA al Ministro del Turismo.

COMUNÍQUESE a los Viceministros, a las Direcciones de Regulaciones y Normas, Economía, a la Oficina de Seguridad de Redes Informáticas, a la Oficina de Informatización, a la Empresa de Telecomunicaciones de Cuba, S.A. y al Director General de la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los días 10 del mes de febrero del 2010.

Ramiro Valdés Menéndez
Ministro

RESOLUCIÓN No. 22/2010

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000 cambió la denominación del Ministerio de Comunicaciones por la de Ministerio de la Informática y las Comunicaciones, para desarrollar las tareas y funciones que hasta el presente realizaba el Ministerio de Comunicaciones, así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sidero Mecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 30 de agosto del 2006, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: El Acuerdo No. 2817 de fecha 25 de noviembre de 1994, del Comité Ejecutivo del Consejo de Ministros, faculta a los Jefes de los Organismos de la Administración Central del Estado; a dictar en el límite de sus facultades y competencia, reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del Organismo y en su caso, para los demás organismos, los órganos locales del poder popular, las entidades estatales, el sector cooperativo, mixto, privado y la población.

POR CUANTO: El Acuerdo No. 3736, de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo

del Consejo de Ministros, establece que el Ministerio de la Informática y las Comunicaciones, es el organismo encargado de ordenar, regular y controlar los servicios informáticos y de telecomunicaciones, nacionales e internacionales y otros servicios afines en los límites del territorio nacional; así como, de conjunto con las organizaciones correspondientes, el Acceso a las Redes de Infocomunicaciones con Alcance Global. Además es la Autoridad encargada de evaluar, proponer y otorgar la expedición y revocación de concesiones, autorizaciones, permisos y licencias a operadores y proveedores de servicios informáticos y de telecomunicaciones, privados o públicos, velando por su cumplimiento en el marco de su autoridad.

POR CUANTO: La Resolución Ministerial No. 179 de fecha 7 de octubre del 2008, establece las normas para la organización, funcionamiento y obligaciones del Proveedor de Servicios de Acceso a Internet al Público.

POR CUANTO: El Grupo Empresarial de Turismo Gaviota S.A. ha solicitado autorización para la prestación de servicios de Acceso a Internet al Público, conforme a lo establecido en la referida norma del Por Cuanto Precedente.

POR CUANTO: Para la autorización de este servicio, se ha tenido en cuenta las características del Grupo Empresarial de Turismo Gaviota S.A. y los servicios que presta a personas naturales, así como las condiciones creadas en este, para brindar servicios de Acceso a Internet al Público.

POR TANTO: En el ejercicio de las facultades que me están conferidas,

RESUELVO:

PRIMERO: Autorizar al Grupo Empresarial de Turismo Gaviota S.A., como Proveedor de Servicios de Acceso a Internet al Público, servicios que presta a personas naturales en el territorio nacional a través de sus áreas de Internet.

SEGUNDO: El Grupo Empresarial de Turismo Gaviota S.A., debe brindar los servicios autorizados, cumplimentando lo establecido en la Resolución No.179 de fecha 7 de octubre del 2008, del Ministerio de la Informática y las Comunicaciones.

TERCERO: La Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones queda encargada de controlar el cumplimiento de lo que por la presente se establece.

DÉSE CUENTA al Ministro de las FAR.

COMUNÍQUESE a los Viceministros, a las Direcciones de Regulaciones y Normas, Economía, a la Oficina de Seguridad de Redes Informáticas, Oficina de Informatización, a la Empresa de Telecomunicaciones de Cuba S.A., a la Presidencia Ejecutiva del Grupo Empresarial de Turismo Gaviota S.A. y al Director General de la Agencia de Control y Supervisión del Ministerio de la

Informática y las Comunicaciones así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los días 10 del mes de febrero del 2010.

Ramiro Valdés Menéndez
Ministro

RESOLUCIÓN No. 99/2009

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000, cambio la denominación del Ministerio de Comunicaciones por la de Ministerio de la Informática y las Comunicaciones, que desarrollará las tareas y funciones que hasta el presente realizaba el Ministerio de Comunicaciones, así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sidero Mecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 30 de agosto del 2006, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: El Acuerdo No. 2817 de fecha 25 de noviembre de 1994, del Comité Ejecutivo del Consejo de Ministros, faculta a los Jefes de los Organismos de la Administración Central del Estado; dictar en el límite de sus facultades y competencia, reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del organismo; y, en su caso, para los demás organismos, los órganos locales del poder popular, las entidades estatales, el sector cooperativo, mixto, privado y la población.

POR CUANTO: El Acuerdo No. 3736, de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo del Consejo de Ministros, establece que el Ministerio de la Informática y las Comunicaciones, es el organismo encargado de ordenar, regular y controlar los servicios informáticos y de telecomunicaciones, nacionales e internacionales y otros servicios afines en los límites del territorio nacional, así como de conjunto con las organizaciones correspondientes, el Acceso a las Redes de Infocomunicaciones con Alcance Global. Además, está encargado de evaluar, proponer y otorgar la expedición y revocación de concesiones, autorizaciones, permisos y licencias a operadores y proveedores de servicios informáticos y de telecomunicaciones, privados o públicos, velando por su cumplimiento en el marco de su autoridad.

POR CUANTO: La Resolución Ministerial No. 179 de fecha 7 de octubre del 2008, ordena en el país todo lo referente a los Proveedores de Servicios de Acceso a Internet al Público.

POR CUANTO: La Empresa Correos de Cuba, cumpliendo con lo dispuesto en la Resolución Ministerial No. 179/ 2008 antes mencionada, ha solicitado autorización para la prestación de Servicios de Acceso a Internet al Público.

POR TANTO: En el ejercicio de las facultades que me están conferidas,

RESUELVO:

PRIMERO: Autorizar a la Empresa Correos de Cuba, como Proveedor de Servicios de Acceso a Internet al Público, los cuales deberá prestar a personas naturales en el territorio nacional a través de sus áreas de Internet.

SEGUNDO: La Empresa Correos de Cuba, brindará los servicios autorizados, conforme se estipula en la Resolución Ministerial No. 179/2008, que establece las normas para la organización, funcionamiento y obligaciones del Proveedor de Servicios de Acceso a Internet al Público.

TERCERO: La Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, queda encargada de controlar el cumplimiento de lo que por la presente se dispone.

NOTIFIQUESE al Presidente de la Empresa Correos de Cuba.

COMUNIQUESE a los Viceministros, a la Agencia de Control y Supervisión, a las Direcciones de Regulaciones y Normas, Economía, Oficina de Seguridad para las Redes Informáticas, a la Empresa de Telecomunicaciones de Cuba S.A., así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHIVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLIQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los días 17 del mes de junio del 2009.

Ramiro Valdés Menéndez
Ministro

4. SEGURIDAD

RESOLUCIÓN No. 58/2022

POR CUANTO: La Ley 149 “De Protección de Datos Personales”, de 14 de mayo de 2022 establece los principios, procedimientos y definiciones fundamentales para garantizar a la persona natural el derecho a la protección de sus datos personales que consten en registros, ficheros, archivos, bases de datos, u otros medios técnicos de tratamiento de datos, sean físicos o digitales de carácter públicos o privados.

POR CUANTO: El avance del proceso de informatización de la sociedad y el incremento del tratamiento automatizado de datos personales en el país, hacen necesario complementar la legislación vigente en materia de seguridad de las Tecnologías de la Información y la Comunicación, con una normativa que regule los requerimientos de seguridad en el tratamiento de datos personales en soporte electrónico.

POR TANTO: En el ejercicio de las atribuciones que están conferidas, en el Artículo 145 inciso d) de la Constitución de la República de Cuba en relación con el Artículo 24 inciso l) numeral 1, del Anexo Único de la Resolución 1, de 7 de agosto de 2017, del Consejo de Ministros;

RESUELVO

ÚNICO: Aprobar el siguiente:

REGLAMENTO PARA LA SEGURIDAD Y PROTECCIÓN DE LOS DATOS PERSONALES EN SOPORTE ELECTRÓNICO

ARTÍCULO 1. El objetivo del presente Reglamento es establecer los requerimientos para la seguridad y protección de los datos personales en soporte electrónico.

ARTÍCULO 2. Este Reglamento es aplicable a los operadores y proveedores de servicios públicos de Telecomunicaciones y las Tecnologías de la Información y la Comunicación, a los de alojamiento y hospedaje, a los de aplicaciones y a los titulares de redes privadas, así como a los que desarrollan actividades relacionadas con el tratamiento de datos personales en soporte electrónico, en lo adelante, responsables y encargados de registros, ficheros, archivos y bases de datos.

ARTÍCULO 3. De conformidad con lo establecido en la Ley 149 “De Protección de Datos Personales”, se considera tratamiento de datos personales en soporte electrónico a las operaciones y procedimientos sistemáticos que permiten la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como su cesión a terceros a través de

comunicaciones, consultas, interconexiones y transferencias, cuando se realizan mediante el uso de las telecomunicaciones y las Tecnologías de la Información y la Comunicación.

ARTÍCULO 4. Los responsables y encargados de registros, ficheros, archivos y bases de datos deben:

a) Garantizar la seguridad y protección de los datos personales en soporte electrónico como parte de la prestación de sus servicios;
b) establecer las medidas técnicas y administrativas necesarias que garanticen un tratamiento de los datos personales en soporte electrónico conforme a lo establecido en el presente Reglamento y demás regulaciones vigentes; y
c) notificar a las autoridades competentes de la ocurrencia de incidentes de ciberseguridad sobre los datos personales en soporte electrónico bajo su custodia.

ARTÍCULO 5. Los responsables y encargados de registros, ficheros, archivos y bases de datos son los únicos autorizados a gestionar programas o aplicaciones informáticas relacionadas con las bases de datos que contienen datos personales en soporte electrónico.

ARTÍCULO 6. Los responsables del registro, fichero, archivo y base de datos tienen las obligaciones siguientes:

a) Crear las vías para que el titular de los datos personales en soporte electrónico, su apoyo o representante legal pueda acceder, modificar y cancelar éstos en el momento en que lo determine, con la mayor brevedad y transparencia posibles;
b) establecer la cancelación de los datos personales en soporte electrónico a solicitud de su titular, su apoyo o representante legal o cuando se haya cumplido el propósito para el cual fueron recopilados, siempre que no se viole lo regulado en ley específica o que estos requieran ser conservados por motivos legales, administrativos, históricos o de otra índole y adoptar las medidas técnicas necesarias para la supresión de cualquier enlace a estos datos y copia;
c) definir los términos y condiciones referidos al uso de los datos personales en soporte electrónico, que deben ser comprensibles por cualquier usuario y establecer las vías para que confirme su aprobación de acuerdo con las características de la base de datos y del servicio;
d) mantener la confidencialidad e integridad de los datos personales en soporte electrónico y evitar su acceso, modificación o transferencia no autorizada; y
e) garantizar el respaldo de los datos personales en soporte electrónico.

ARTÍCULO 7. Los responsables y encargados solamente pueden hospedar o replicar los registros, ficheros, archivos y bases de datos en soporte electrónico, que contienen datos personales, en servidores nacionales ubicados en el país, salvo los casos previstos en la Ley.

ARTÍCULO 8. Los términos y condiciones de uso del servicio se aplican de acuerdo con lo establecido en la Ley 149 “De Protección de Datos Personales” y las características de la base de datos y del servicio en particular e incluyen los aspectos siguientes:

a) Informar al usuario el propósito de la recopilación de datos personales al momento de su solicitud, dónde estos son almacenados y el plazo de tiempo por el cual son conservados al cumplir su finalidad;
b) describir las opciones que le permiten al titular de los datos gestionar su privacidad;
c) alertar al usuario sobre el uso de elementos en el sitio web que puedan ser utilizados para rastrear su actividad, como cookies, incluso si son aplicados por terceros;
d) comunicar al usuario con al menos 3 meses de antelación las modificaciones que se realicen al texto de los términos y condiciones, mediante correo electrónico, SMS, notificación en el programa y aplicación informática, sitio web u otros; y
e) establecer el plazo mínimo para la cancelación de los datos personales en soporte electrónico, el cual no debe ser mayor a lo dispuesto en la legislación vigente en la materia.

ARTÍCULO 9. 1. Los datos personales en soporte electrónico se pueden utilizar con objetivos académicos, investigativos o sociales, con técnicas de análisis de datos, siempre que sean anonimizados o disociados y su recolección solo incluya los datos mínimos necesarios para cumplir su propósito.

2. El intercambio de información para la realización de estos objetivos, se debe realizar de manera contractual entre el responsable de la base de datos y el que utiliza los datos y cumplir lo establecido en la presente Resolución.
3. El intercambio de los datos anonimizados o disociados con otra entidad para utilizarlos con los objetivos expresado en el apartado 1 de este artículo, se realiza sin interés comercial.

ARTÍCULO 10. Los titulares de datos personales en soporte electrónico, que sean usuarios de servicios públicos de telecomunicaciones, programas y aplicaciones informáticas y de redes sociales y servicios de Internet ofrecidos por entidades nacionales, tienen los derechos siguientes:

a) Conocer el propósito para el cual son solicitados sus datos y el uso que se les da a estos;
b) acceder, actualizar y cancelar en el momento en que estos lo consideren, los datos personales facilitados para el uso del servicio;
c) que sus datos sean cancelados cuando así lo estimen conveniente, se haya cumplido el propósito para el cual fueron recopilados o cuando consideren que se están tratando de forma que vulnere sus intereses y derechos; y
d) ser informados sobre las opciones de configuración de privacidad disponibles que les permitan determinar cómo su información es tratada, compartida y almacenada.

DISPOSICIONES FINALES

PRIMERA: La Dirección General de Informática, la Dirección de Inspección y las oficinas territoriales de control del Ministerio de Comunicaciones, quedan encargadas según corresponda, de controlar el cumplimiento de lo dispuesto en la presente Resolución.

SEGUNDA: La presente Resolución entra en vigor a los 180 días posteriores de su publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE al Director General de Informática, a la Directora de Inspección y los directores territoriales de control, del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, al Director General de Comunicaciones, al Director de Regulaciones, todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los 19 días del mes de agosto de 2022.

Wilfredo González Vidal

RESOLUCIÓN No. 105/2021

POR CUANTO: El Decreto 360 “Sobre la Seguridad de las Tecnologías de la Información y la Comunicación para la informatización de la sociedad y la Defensa del Ciberespacio Nacional” de 31 de mayo del 2019 en su Artículo 25 inciso d), regula que el Ministerio de Comunicaciones en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, establece el Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad y asegura los procedimientos para su implementación en todos los niveles por parte de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, así como realiza el enfrentamiento y neutralización de estos sucesos de acuerdo a lo que a cada organismo le corresponde.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO SOBRE EL MODELO DE ACTUACIÓN NACIONAL PARA LA RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. El presente Reglamento tiene por objeto establecer el Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad en el ámbito del Ciberespacio Nacional y con ello garantiza una respuesta efectiva para su protección.

Artículo 2. Este Reglamento es de aplicación para las personas naturales y jurídicas, se considera en estos últimos los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales, los órganos del Poder Popular, las sedes diplomáticas y en las representaciones comerciales y de cooperación que Cuba posee en el exterior, el sistema empresarial y las unidades presupuestadas, las cooperativas, las empresas mixtas, demás modalidades de inversión extranjera, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas y los titulares de redes de datos en el Ciberespacio Nacional.

Artículo 3. Se entiende por respuesta a un incidente de Ciberseguridad, a todo el proceso que se realiza para su gestión.

CAPÍTULO II
OBJETIVOS Y PRINCIPIOS DE FUNCIONAMIENTO

Artículo 4. Los objetivos del Modelo de Actuación para la respuesta a incidentes de Ciberseguridad son los siguientes:

a) Garantizar a través de la gestión de incidentes de Ciberseguridad**,** se pueda prevenir, detectar y responder oportunamente ante posibles actividades enemigas, delictivas y nocivas que puedan ocurrir en el ciberespacio, así como realizar el enfrentamiento y neutralización de estos sucesos y atender a lo que a cada organismo que participan en la seguridad de las Tecnologías de la Información y la Comunicación, en lo adelante TIC, le corresponde;
b) coordinar la actuación oportuna, ordenada y efectiva de las personas jurídicas mencionadas en el Artículo 2, involucradas en un incidente y su intervención en cada una de las etapas;
c) evaluar el daño causado y minimizar sus consecuencias;
d) establecer la cooperación entre los organismos que participan en la seguridad de las TIC y la defensa del Ciberespacio Nacional;
e) adoptar una terminología común para clasificar los incidentes de Ciberseguridad.

Artículo 5. El reporte y gestión de los incidentes de Ciberseguridad se organiza en correspondencia con las competencias de los organismos que participan en la seguridad de las TIC y la defensa del Ciberespacio Nacional, la categorización de los sistemas de trabajo y actividades, así como los sistemas de clasificación que al respecto se implementen.

Artículo 6. La actuación ante un incidente de Ciberseguridad se realiza por etapas, con

independencia de la clasificación de este, y se ejecutan a todos los niveles las acciones comprendidas en cada una, las que se definen en el Anexo I del presente Reglamento; se establecen como obligatorias las siguientes:

a) Etapa 1: Prevención y Protección: Se refiere a las acciones preventivas y de protección de carácter extensivo que coadyuvan y contribuyen a evitar incidentes cibernéticos que pueden impactar en la Ciberseguridad.
b) Etapa 2: Detección, Evaluación y Notificación: Se refiere a todo el proceso en que se detecta, se evalúa su impacto y se notifica el incidente.
c) Etapa 3: Investigación: Incluye el proceso de esclarecimiento del incidente de acuerdo a las competencias de los organismos que participan en la seguridad de las TIC y la defensa del Ciberespacio Nacional.
d) Etapa 4: Mitigación y Recuperación: Incluye las acciones organizativas y tecnológicas que permitan remediar los daños causados, mitigar las vulnerabilidades que propiciaron la ocurrencia del incidente, la recuperación y el seguimiento a las medidas tomadas.

CAPÍTULO III
CLASIFICACION DE LOS INCIDENTES DE CIBERSEGURIDAD Y CATEGORIZACIÓN DE LOS SISTEMAS DE TRABAJO

Artículo 7. Se considera un incidente de Ciberseguridad cualquier evento que se produzca de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de la información y la comunicación o los procesos que con ellas se realizan.

Artículo 8. Se entiende por evento de Ciberseguridad al cambio en el estado de un sistema o servicio, que puede generar una alerta o notificación creada por un elemento de configuración, servicio o herramienta de monitorización.

Artículo 9. Se define como peligrosidad la potencial amenaza que supondría la materialización de un incidente en los sistemas y servicios TIC, fundamentada en las características intrínsecas a la tipología de la amenaza y su comportamiento.

Artículo 10. Para la clasificación de incidentes de Ciberseguridad se tiene en cuenta:

a) La tipificación del incidente;
b) el nivel de peligrosidad para la organización.

Artículo 11. **1.** La tipificación de los incidentes de Ciberseguridad se realiza con el objetivo de facilitar su caracterización, se agrupan por categorías y subcategorías;
2. La caracterización de la peligrosidad de los incidentes de Ciberseguridad se utiliza una escala de 4 niveles que son:

a) Baja,
b) media;
c) alta;
d) muy alta.

3. Tanto la tipificación de los incidentes como la caracterización de la peligrosidad, se describen en el

Anexo II de la presente Resolución.

Artículo 12. El impacto de un incidente de Ciberseguridad en las infraestructuras y servicios TIC, se determina por las consecuencias potenciales que ha tenido, o por la categorización de los sistemas y se tiene en cuenta la jerarquía y el papel que desempeñan los sujetos afectados.

Artículo 13. Se define como categorización de los sistemas y actividades, al orden de prioridad que se establece para la adopción de esquemas de seguridad diferenciados en correspondencia con la confidencialidad, integridad y disponibilidad de la información y los servicios.

Artículo 14. El esquema de seguridad son los lineamientos conceptuales para prevenir, detectar, mitigar y responder a los fenómenos del Ciberespacio con impacto en la información, los servicios y sus tecnologías asociadas.

Artículo 15. Los sistemas y actividades se categorizan en cuatro niveles de seguridad: máxima, alta, media y básica; fundamentada según el impacto en las áreas de alta importancia nacional.

Artículo 16. Se considera de máxima seguridad el nivel en el que prevalecen informaciones y servicios relacionados con objetivos estratégicos de la defensa, políticos, económicos, científico-técnicos y sociales y que su divulgación o conocimiento no autorizado o su alteración o insuficiente disponibilidad, puedan producir o produzca daños excepcionalmente graves.

Artículo 17. Se considera de alta seguridad el nivel en el que prevalecen informaciones y servicios relacionados con objetivos de la defensa, políticos, económicos, científico-técnicos y sociales y que su divulgación o conocimiento no autorizado o su alteración o insuficiente disponibilidad, puedan producir o produzca serios daños o que generen condiciones para alterar el orden público.

Artículo 18. Se considera de seguridad media el nivel en el que prevalecen informaciones y servicios relacionados con objetivos de la defensa, políticos, económicos, científico-técnicos y sociales y que su divulgación o conocimiento no autorizado o su alteración o insuficiente disponibilidad, puedan producir o produzca daños o ser perjudicial.

Artículo 19. Se considera de seguridad básica el nivel en el que prevalecen informaciones y servicios relacionados con el ciudadano u otros objetivos sensibles para el encargo estatal de la estructura.

CAPÍTULO IV
ACTUACIÓN ANTE LOS INCIDENTES DE CIBERSEGURIDAD

Artículo 20. 1. La actuación ante un incidente de Ciberseguridad se rige por lo expresado en el Artículo 6.
2. La prioridad y actuación ante un incidente es según se indica en la siguiente tabla:

Nivel de Peligrosidad / Nivel de Seguridad	Muy Alto	Alto	Medio	Bajo
Máxima	1	1	2	2
Alta	1	2	3	3
Media	2	3	3	4
Básica	3	3	4	4

Artículo 21. Los titulares de redes privadas de datos son responsables de que los eventos e incidentes de Ciberseguridad, sean registrados, clasificados y de entregar la información según lo que establece el artículo 22; así como que los especialistas que gestionan las infraestructuras y servicios se encuentren capacitados para ejecutar las acciones correspondientes a cada etapa.

Artículo 22. Los responsables vinculados directamente a la informática en las infraestructuras donde ocurran incidentes de Ciberseguridad están obligados a informar al Jefe inmediato superior y al Equipo de Respuesta a Incidentes Computacionales de Cuba, denominado CuCERT perteneciente a la Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones, para lo cual en el Anexo III se define el contenido informativo que se envía a la mencionada organización; quien ratifica o reclasifica el incidente de conjunto con las entidades especializadas, e informa a la entidad afectada si este varia.

Artículo 23. Los incidentes de Ciberseguridad que sean detectados por fuentes ajenas a la entidad afectada, una vez conocido por la Oficina de Seguridad para las Redes Informáticas se notifica a dichas entidades, las que actúan según lo establecido.

SEGUNDO: Los titulares de las redes privadas de personas naturales, y las personas naturales individualmente, informan los incidentes de Ciberseguridad por las vías que establezca el Ministerio de Comunicaciones, lo cual se comunica a través de su sitio web.

DISPOSICIONES ESPECIALES

PRIMERA: Se faculta a la Dirección de Ciberseguridad perteneciente al Ministerio de Comunicaciones en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias y del Interior para implementar las acciones complementarias que se requieran para dar cumplimiento a lo que por la presente Resolución se dispone.

SEGUNDA: Los Ministerios de las Fuerzas Armadas Revolucionarias y del Interior adecuan hacia sus sistemas internos, lo establecido en el presente Reglamento, de conformidad con sus estructuras y funciones.

TERCERA: El Equipo de Respuesta a Incidentes Computacionales de Cuba, denominado CuCERT perteneciente a la Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones,

recibe y envía la información sobre incidentes de Ciberseguridad referida en los Artículos 22 y 23 respectivamente, hasta tanto se cree la entidad especializada de Ciberseguridad con la participación conjunta de los ministerios de Comunicaciones, de las Fuerzas Armadas y del Interior para atender estos incidentes.

DISPOSICIÓN FINAL

ÚNICA: Los directores generales de Informática, de la Oficina de Seguridad para las Redes Informáticas y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, el director de Inspección del Ministerio de Comunicaciones y las oficinas territoriales de control, quedan encargados, según corresponda, del control del cumplimiento de lo que por la presente se dispone.

NOTIFÍQUESE al viceministro que atiende al área de Informática, a los directores generales de Informática, al de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y al de la Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Defensa y de Comunicaciones y a los directores de Regulaciones, de Inspección y a los territoriales de control, todos del Ministerio de Comunicaciones.

DÉSE CUENTA a los ministros de la Fuerzas Armadas Revolucionarias y del Interior.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 9 días del mes de agosto de 2021.

Mayra Arevich Marín

Anexo I

ACCIONES A EJECUTAR EN LAS DIFERENTES ETAPAS ANTE UN INCIDENTE DE CIBERSEGURIDAD

Etapa 1: Prevención y Protección

En esta etapa se incluyen:

1. Establecer las bases normativas regulatorias para garantizar la implementación de las políticas de Ciberseguridad.

2. Garantizar el diseño, establecimiento, control y mejora continua de las medidas de protección que permitan la prevención, detección, contención y respuesta ante la ocurrencia de incidentes.
3. Compatibilizar, homologar y certificar la seguridad de las infraestructuras y servicios, según su propósito y clasificación de acuerdo con la legislación vigente.
4. Promover el desarrollo de soluciones integradas, protegidas y propias para la seguridad tecnológica.
5. Realizar ejercicios de Ciberseguridad para la comprobación de las capacidades reactivas, tanto organizativas como tecnológicas, ante posibles incidentes.
6. Implementar, como parte de la cooperación nacional, el intercambio con entidades especializadas en materia de Ciberseguridad.
7. Realizar campañas comunicacionales para fomentar la cultura de Ciberseguridad y elevar la percepción de riesgo.

Etapa 2: Detección, evaluación y notificación
En esta etapa se realizan las acciones siguientes:

1. Realizar una evaluación preliminar del daño y de las causas y condiciones que ocasionaron o propiciaron el incidente, realizar la clasificación del incidente según peligrosidad, de acuerdo con lo establecido en la presente resolución.
2. Preservar las evidencias digitales del lugar del hecho, y las informaciones sobre los eventos de seguridad detectados por los sistemas de supervisión existentes. Esto puede incluir el aislamiento del objeto afectado de la infraestructura y la paralización parcial o completa de servicios.
3. Notificación a los niveles correspondientes de acuerdo con el Artículo 22.
4. Analizar y recolectar, para su revisión posterior, todos los eventos registrados por los sistemas de supervisión, los resultados de auditorías, diagnósticos integrales y ejercicios de Ciberseguridad efectuados. Buscar antecedentes del hecho.
5. Dar seguimiento al flujo informativo en las sucesivas etapas del modelo.

Etapa 3: Investigación
En esta etapa se ejecutan las acciones siguientes:

1. Comprobar el incidente, a través de la caracterización del fenómeno, se identifican las causas y condiciones.
2. Realizar análisis retrospectivos para la reconstrucción de los hechos, así como la ejecución de diagnósticos reactivos para complementar las investigaciones.
3. Generar hipótesis sobre el hecho para su posterior comprobación y validación.
4. Determinar la responsabilidad administrativa, jurídica y penal, cuando corresponda, sobre el hecho investigado.

5. Documentar y legalizar los elementos probatorios que permitan establecer la identidad y objetivos, víctimas y modo de operar.
6. Informar a los niveles superiores de las personas jurídicas involucradas en el incidente sobre los daños y su repercusión política, económica y social, así como el impacto tecnológico y sus consecuencias.

Etapa 4: Mitigación y recuperación

Esta etapa comprende las siguientes acciones:

1. Diseñar e implementar soluciones tecnológicas para su erradicación.
2. Resolver las problemáticas detectadas en el estudio de causas y condiciones que permitieron que el ataque fuera efectivo.
3. Evaluar la pertinencia de restablecer gradualmente los entornos afectados, y restablecerlos en tanto no entorpezcan el curso de la investigación.
4. Notificar por el órgano encargado de la gestión de la Ciberseguridad del Ministerio de Comunicaciones a las instituciones externas al país implicadas en el incidente, y se solicita su posición oficial, cuando corresponda.

Anexo II

TIPIFICACIÓN DE LOS INCIDENTES DE CIBERSEGURIDAD Y NIVEL DE PELIGROSIDAD

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
1. Daños éticos y sociales	1. Eco mediático de noticias falsas	Divulgación de noticias falsas, mensajes ofensivos, difamación con impacto en el prestigio del País.	Alto
	2. Bloqueos masivos de cuentas en Redes sociales	Afectaciones masivas a cuentas.	Alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	3. Difusión dañina	Difusión a través de las infraestructuras, plataformas o servicios de telecomunicaciones /TIC, de contenidos que atentan contra los preceptos constitucionales, sociales y económicos del estado, incite a movilizaciones u otros actos que alteren el orden público; difundan mensajes que hacen apología a la violencia, accidentes de cualquier tipo que afecten la intimidad y dignidad de las personas.	Alto
2. Desastres naturales	Terremotos, inundaciones, huracanes, relámpagos (descarga eléctrica), tsunamis, derrumbes, aludes y otros desastres	Interrupción o destrucción, parcial o total de la infraestructura informática de comunicación, de telecomunicaciones o comprometimiento de la seguridad de la información debido a desastres naturales.	Muy Alto
3. Incidentes de agresión	1. Ciberterrorismo	Acciones mediante el uso de las TIC cuya finalidad es subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas y de masas, las estructuras económicas y sociales del estado, u obligar a los poderes públicos a realizar un acto o abstenerse de hacerlo. Alterar gravemente la paz pública. Desestabilizar gravemente el funcionamiento de una organización internacional. Provocar un estado de terror en la población o en una parte de ella.	Muy alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	2. Ciberguerra	Métodos de Guerra no Convencional y acciones ofensivas de carácter militar empleados para derrocar el gobierno mediante el uso de las TIC con desarrollo de ataques cibernéticos a infraestructuras críticas para justificar acciones políticas, económicas, subversivas o de injerencia.	Muy Alto
	3. Subversión social	Pretender alterar el orden público, promover la indisciplina social	Muy Alto
4. Contenido dañino	Fraude	Acción que resulta contraria a la verdad y a la rectitud que perjudica a personas e instituciones del Estado.	Muy alto
5. Incidentes contra la dignidad y la individualidad	1. Pornografía	Difusión y distribución a través de las TIC de materiales pornográficos.	Medio

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	2. Ciberacoso	Uso de las TIC con la intención de acosar u hostigar a una persona, o grupo de personas, mediante ataques personales, divulgación de información privada, íntima o falsa. Intenta obligar a una persona natural o jurídica, mediante el empleo de violencia o intimidación, a realizar u omitir actos con la intención de producir un perjuicio a ésta, o bien con ánimo de lucro de la que lo provoca. Comunicaciones no esperadas o deseadas, así como acciones o expresiones que lesionan la dignidad de otra persona, que menoscaban su fama o atentan contra su propia estimación.	Medio
	3. Engaño pederasta (Grooming)	Cualquier comportamiento a través de las TIC relacionado con la captación o utilización de menores de edad o personas con discapacidad necesitadas de especial protección, con el objetivo de ganarse su amistad para realizar actos que atenten contra su indemnidad o libertad sexual.	Alto
6. Daños físicos	1. Afectaciones en el sistema de comunicaciones por fuego, escapes de gas o agua, polución, corrosión, roturas de cables accidentes automovilístico, o aéreo y otras causas.	Acciones físicas deliberadas o accidentales que causan daños o destrucción de las telecomunicaciones/TIC.	Alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	2. Robo de equipamiento informático	Robo de equipamiento informático	Alto
7. Acción no autorizada	1. Uso no autorizado de recursos	Empleo de tecnologías y servicios asociados a las TIC por usuarios que no están debidamente autorizados por la dirección competente. Acceso lógico o físico a un equipo, sistema, aplicación, datos o cualquier recurso técnico, la utilización ilegal de frecuencia del espacio radioeléctrico para afectar equipos o sistemas vitales.	Medio
	2. Servicio de TIC ilegal	Establecer un servicio TIC sin la correspondiente autorización de la dirección competente.	Alto
	3. Instalación de software no permitido	Instalación de cualquier software en la infraestructura informática de la organización, no contemplado en el Plan de Seguridad y sin el conocimiento de la dirección competente.	Medio
	4. Acceso no autorizado a la administración de sitios web	Proceso por el cual un usuario accede sin estar autorizado, y vulnera la seguridad del sitio web.	Medio
8. Fallas de la infraestructura	1. Fallo de Climatización	Cualquier tipo de fallo en los dispositivos de clima que interrumpa el funcionamiento, parcial o total, de la infraestructura de TIC.	Medio
	2. Fallo eléctrico	Cualquier tipo de fallo eléctrico que interrumpa el funcionamiento, parcial o total, de la infraestructura TIC	Medio

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
9. Fallas Técnicas	1. Fallo del equipamiento	Cualquier tipo de fallo que interrumpa el funcionamiento, parcial o total, de la infraestructura TIC.	Muy Alto
	2. Fallo de aplicaciones o servicios	Cualquier tipo de falla causada por el mal funcionamiento de un programa o servicio que interrumpa el funcionamiento, parcial o total, de la infraestructura TIC.	Muy Alto
	3. Plataformas desactualizadas	Aplicaciones web cuya plataforma se encuentra desactualizada y con presencia de vulnerabilidades.	Medio
10. Interferencias	1. Radiaciones, pulsos electromagnéticos y otras interferencias	Interferencia provocada o generada desde el interior del país, a uno o varios de los sistemas radioeléctricos. Interferencia provocada o generada desde el exterior del país, a equipos y sistemas, que pueden soportar o no la gestión de infraestructuras críticas. Emisiones causadas por equipos radioeléctricos, con manipulación o no de sus parámetros sin una continua verificación, los cuales pueden provocar un deterioro del servicio o interferencias perjudiciales a otros sistemas en uso, o pueden ser utilizados para provocar daños intencionadamente.	Muy Alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	2. Cambios de características de aplicaciones, equipos o componentes y servicios	Cambios de características de aplicaciones, equipos o componentes y servicios sin la autorización de la dirección competente. Cambios o intentos de modificación de la infraestructura o de equipamiento que use el espectro radioeléctrico y provoque interferencias.	Medio
11. Compromiso de la Información	1. Borrado o modificación de información	Proceso por el cual un usuario no autorizado accede a borrar o modificar contenido para el cual no está autorizado.	Alto
	2. Publicación o pérdida de información oficial clasificada	Proceso por el cual un usuario difunde información clasificada a través de canales no previstos o autorizados para compartir esa información.	Alto
	3. Pérdida de datos e información	Proceso por el cual, por comisión u omisión se pierden datos e información.	Alto
	4. Robo de información	Proceso por el cual un usuario no autorizado, interno o externo a la entidad, se apropia de información mediante las TIC.	Alto
	5. Sniffers	Análisis mediante software del tráfico de una red con la finalidad de capturar información. El tráfico que viaje no cifrado puede ser capturado y usado para detectar y analizar posibles vulnerabilidades.	Medio

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	6. Hombre en el medio	Método mediante el cual el atacante se sitúa entre las dos partes que intentan comunicarse; intercepta los mensajes enviados e imita al menos a una de ellas. Análisis local o remoto mediante software, de puertos, redes y tecnologías informáticas.	Alto
	7. Pruebas o escaneos ilegales	Pruebas realizadas por parte de estaciones radioeléctricas o escaneos con el objetivo de encontrar brechas o vulnerabilidades en la seguridad de una infraestructura de TIC.	Medio
	8. Ingeniería Social	Técnicas que buscan la revelación de información sensible asociadas a las TIC de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.	Alto
	9. Phishing	Suplantación de la identidad mediante las TIC en la cual el atacante, trata de obtener información relevante de los usuarios para uso dañino.	Medio
12. Comercialización Ilegal	Comercialización ilegal de productos de software o hardware y servicios de redes	Proceso por el cual un usuario, contraviene las disposiciones vigentes o internas de una organización, e introduce en las redes o comercializa software o hardware no autorizados.	Medio
13. Correos no deseados	1. Cadenas	Correo que busca coaccionar o convencer a sus destinatarios, para que sea reenviado a otro grupo de usuarios de correo electrónico.	Bajo

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	2. Hoax	Correo electrónico con una noticia falsa o parcialmente real, enviada con el objeto de engañar al destinatario, y trata que éste crea que todo el mensaje es real.	Bajo
	3. Spam	Correo no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados a un mismo usuario en un corto período.	Bajo
14. Desfiguración de Sitios Web	1. Inclusión local o remota de ficheros	Acción que permite a un atacante ejecutar archivos remotos alojados en otros servidores a causa de una mala configuración del sitio web y que provoque pérdida o modificación de la información.	Alto
	2. Inyección de código	Introducción de cadenas mal formadas, o cadenas que el receptor no espera o controla debidamente; las cuales provocan que sea modificada o destruida la información.	Alto
15. Compromiso de las funciones	1. Derecho de autor	Violación de derechos de propiedad intelectual al compartir a través de las TIC materiales en formato digital y software.	Alto
	2. Robo de credenciales	Proceso a través del cual un tercero se apropia de las credenciales de acceso de una cuenta que no le pertenece para uso indebido.	Alto
	3. Suplantación de identidad	Técnica de simulación de personas jurídicas o naturales. Intentos fraudulentos para adquirir información sensible, provocar daños o penetrar un sistema informático, una infraestructura o servicio de TIC con el objetivo de facilitar o realizar un delito.	Alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
16. Programas malignos	1. Amenaza persistente avanzada (APT)	Conjunto de procesos informáticos sigilosos y continuos de piratería informática, a menudo orquestada por humanos, dirigido a una entidad específica.	Muy Alto
	2. Robot informáticos (Botnet)	Conjunto de máquinas controladas remotamente con finalidad generalmente maliciosa. Un BOT es una pieza de software maliciosa que recibe órdenes de un atacante principal que controla remotamente la máquina.	Alto
	3. Gusanos	Código maligno similar a un virus, y en ocasiones se considera una subclasificación del mismo, con la capacidad de diseminarse sin la necesidad de una acción humana mediante la explotación de vulnerabilidades del Sistema Operativo o de contraseñas débiles.	Alto
	4. Secuestro de la Información (Ransomware)	Código maligno que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.	Muy Alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	5. Troyanos	Código maligno que se enmascara como software legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. Una vez instalado, el software dañino tiene la capacidad de desarrollar actividad perjudicial en segundo plano. Un troyano no depende de una acción humana y no tiene la capacidad de replicarse, no obstante puede tener gran capacidad dañina en un sistema a modo de troyanos o explotan vulnerabilidades de software.	Alto
	6. Tráfico con C&C (Mando y Control)	Paneles de mando y control (también referenciados como C2), por el cual atacantes Cibernéticos controlan determinados equipos zombie infectados con muestras de la misma familia de software dañino. El panel de comando y control actúa como punto de referencia, control y gestión de los equipos infectados.	Alto
	7. Virus Informático	Es un tipo de código maligno cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de software, archivos o documentos con carga dañina, adquiere la capacidad de replicarse de un sistema a otro.	Alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	8. Programas Espías (Spyware)	Código maligno que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir keyloggers, monitorizaciones, recolección de datos, así como robo de datos.	Alto
	9. Rootkit	Conjunto de software dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones.	Alto
	10. Dialer	Código maligno que se instala en una máquina y, de forma automática y sin consentimiento del usuario, realiza marcaciones telefónicas a número de tarifa especial.	Alto
17. Ataques técnicos o Intrusión	1. Denegación de Servicio (DoS)	Consiste en una serie de técnicas que provocan la inoperatividad de un servicio o un recurso. El procedimiento consiste en la implementación masiva de peticiones a un servidor, lo que genera una sobrecarga del servicio y el posterior colapso del mismo al no poder éste atender la gran cantidad de solicitudes que le llegan.	Alto
	2. Denegación de Servicio Distribuido(DDoS)	Se trata de una variante de DoS en el que la remisión de peticiones se lleva a cabo de forma coordinada desde varios puntos hacia un mismo destino. Para ello se emplean redes de bots, generalmente sin el conocimiento de los usuarios.	Muy Alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	3. Ataque por fuerza bruta	Proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de combinaciones alfanuméricas, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.	Alto
	4. Explotación de Vulnerabilidades	Consiste en cualquier práctica mediante la cual un atacante Cibernético, aprovecha vulnerabilidades de un sistema de información y/o comunicación, con fines ilícitos y para los cuales no está debidamente autorizado.	Muy Alto
	5. Cambios de características del Hardware	Cambios de características del hardware sin la autorización de la dirección competente. Cambios o intentos de modificación de la infraestructura o de equipamiento que use el espectro radioelectrónico.	Alto
	6. Cambios de características del Software o Base de Datos.	Cambios de características del software y/o Base de Datos, sin la autorización de la dirección competente.	Medio
	7. Manipulación de DNS	Uso de técnicas para la recolección de información acerca de la infraestructura y subdominios de un objetivos.	Alto

Anexo III

MODELO DE INFORMACIÓN PARA REPORTAR LOS INCIDENTES DE CIBERSEGURIDAD

DATOS DEL INFORMANTE				
Nombre y apellidos:				
Organismo:	Entidad:	Cargo:		
Dirección:		Provincia:	Municipio:	País:
Correo electrónico:	Teléfono donde contactar:	Fax:		
Vía del reporte:	Fecha:	Hora:		
Otros datos de interés:				
DATOS DE LA ENTIDAD AFECTADA				
Organismo:	Dependencia:	Entidad:		
A quien contactar (Nombre y Apellidos):				
Dirección:		Provincia:	Municipio:	País:
Correo electrónico:	Teléfono:	Fax:		
Otros datos de interés:				
DATOS DEL INCIDENTE				
Categoría del incidente:		Clasificación nivel de Seguridad/peligrosidad en la entidad:		
Fecha de detección:	Hora de detección:	Sistema operativo:		
Origen del Incidente: (si se conoce)				
Descripción del incidente:				
Recursos Afectados:				
Contramedidas aplicadas:		Otra Información de Interés:		

RESOLUCIÓN No. 129/2019

POR CUANTO: El Decreto 360 “Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional” de 5 de junio de 2019 establece en su Artículo 19 que el diseño del Sistema de Seguridad Informática y la elaboración del Plan de Seguridad Informática de cada entidad se realizan en correspondencia con las metodologías establecidas por el Ministerio de Comunicaciones, por lo que se considera necesario establecer la Metodología para la Gestión de la Seguridad Informática en todo el país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar la Metodología para la Gestión de la Seguridad Informática que se anexa y que forma parte integrante de la presente Resolución.

SEGUNDO: Las entidades disponen de ciento ochenta días contados a partir de la entrada en vigor de la presente Resolución, para establecer sus Sistemas de Gestión de la Seguridad Informática, en correspondencia con lo regulado en la referida metodología.

TERCERO: La Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones es la encargada de ejercer el control del cumplimiento de lo dispuesto en la presente Resolución.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas, la Metodología para la Gestión de la Seguridad Informática.

NOTIFÍQUESE al director general de la Oficina de Seguridad para las Redes Informáticas.

COMUNÍQUESE a los viceministros, al director general de Informática y al director de Regulaciones del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los días 24 del mes de junio del 2019.

Jorge Luis Perdomo Di-Lella

ANEXO

METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA

ÍNDICE

implementación del SGSI
- 1.1.3. Recopilar información de seguridad
- 1.2. Determinación de las necesidades de protección
- 1.2.1 Caracterización del sistema informático
- 1.2.2. Identificación de las amenazas sobre el sistema informático
- 1.2.3. Estimación del riesgo sobre los bienes informáticos
- 1.2.4. Evaluación del estado actual de la Seguridad Informática
- 1.3 Establecimiento de los requisitos de Seguridad Informática
- 1.4 Selección de los controles de Seguridad Informática
- 1.4.1. Políticas de Seguridad Informática
- 1.4.2. Medidas y procedimientos de Seguridad Informática
- 1.5. Organización de la Seguridad Informática
- 1.5.1. Organización interna
- 1.5.2. Coordinación de la Seguridad Informática
- 1.5.3. Asignación de responsabilidades sobre Seguridad Informática
- 1.6. Elaboración del Plan de Seguridad Informática

2. Proceso de Implementación del SGSI
   - 2.1. Programa de Desarrollo de la Seguridad Informática
   - 2.2. Factores Críticos de éxito
3. Proceso de Verificación del SGSI
   - 3.1. Métodos de Medición
   - 3.2. Indicadores de medición
   - 3.3 Reglas que cumple una buena métrica
4. Proceso de Actualización del SGSI

Segunda Parte: Estructura y contenido del Plan de Seguridad Informática
1. Alcance del Plan de Seguridad Informática
2. Caracterización del Sistema Informático
3. Resultados del Análisis de Riesgos
4. Políticas de Seguridad Informática
5. Responsabilidades
6. Medidas y Procedimientos de Seguridad Informática
   - 6.1. Clasificación y control de los bienes informáticos
   - 6.2. Del Personal
   - 6.3. Seguridad Física y Ambiental
   - 6.4. Seguridad de Operaciones
   - 6.5. Identificación, Autenticación y Control de Acceso
   - 6.6. Seguridad ante programas malignos
   - 6.7. Respaldo de la Información
   - 6.8. Seguridad en Redes
   - 6.9. Gestión de Incidentes de Seguridad
7. Anexos del Plan de Seguridad Informática
   - 7.1 Listado nominal de Usuarios con acceso a los servicios de red
   - 7.2 Registros
   - 7.3 Control de Cambios

Objeto

La presente metodología tiene por objeto determinar las acciones a realizar en una entidad durante el diseño, la implementación y posterior operación de un Sistema de Gestión de la Seguridad Informática, en lo adelante SGSI, compuesta por dos partes, la primera se dedica al SGSI y la segunda a la estructura y contenido del Plan de Seguridad Informática.

Constituye un complemento a lo exigido en el Decreto de Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional y el Reglamento de Seguridad para las Tecnologías de la Información y la Comunicación en cuanto a la obligación de diseñar, implantar y mantener actualizado un Sistema de Seguridad Informática, a partir de los bienes a proteger y de los riesgos a que están sometidos.

Alcance

Esta metodología está dirigida a todas las personas vinculadas con las Tecnologías de la Información y la Comunicación, en lo adelante TIC, de una entidad, ya sea por la responsabilidad que tienen asignadas en relación con los bienes informáticos o por los beneficios que de ellos obtienen.

Los primeros destinatarios de esta metodología son los directivos y funcionarios de los distintos niveles de una entidad, que responden por el buen funcionamiento de las tecnologías y la información que en ellas se procesa.

Términos y definiciones

A los efectos de la presente metodología se entiende por:

1. **Análisis de riesgos:** proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos, e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.
2. **Identificación de usuarios:** identificador (ID) que define quién es el usuario y qué lo identifica unívocamente en el sistema, diferenciándolo en los sistemas multiusuario del resto.
3. **Impacto:** daño producido por la materialización de una amenaza.
4. **Riesgo residual:** riesgo remanente después de aplicados controles de seguridad para minimizarlo.
5. **Sistema informático:** conjunto de bienes informáticos de que dispone una entidad para su correcto funcionamiento y la consecución de sus objetivos.
6. **Soportes removibles:** cualquier tipo de dispositivo intercambiable que permita la transferencia o almacenamiento de información.
7. **Trazas de auditoría:** registros que se generan para describir la información asociada a eventos de interés en los diferentes procesos que se ejecutan en las TIC; están compuestos por secciones y campos donde se describen aspectos como fecha y hora, tipo de evento, quién o

qué lo causa, y qué se afecta, que permiten comprender el evento que se registra y usualmente se registran en orden cronológico.

El SGSI de una entidad se diseña con la consideración del conjunto de sus bienes informáticos a partir de su importancia y el papel que representan para el cumplimiento de su actividad, por lo que se presta especial atención a aquellos que son críticos en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo a que están sometidos.

Un SGSI conlleva la conformación de una estrategia sobre cómo tratar los aspectos de seguridad e implica la implementación de los controles necesarios para garantizar el cumplimiento de lo establecido en esta materia, a partir de un análisis de riesgos que incluya:

1. determinar qué se trata de proteger;
2. determinar de qué es necesario protegerse;
3. determinar cuan probables son las amenazas;
4. implementar los controles que protejan los bienes informáticos de una manera rentable; y
5. revisar continuamente este proceso y perfeccionarlo cada vez que una debilidad (vulnerabilidad) sea encontrada.

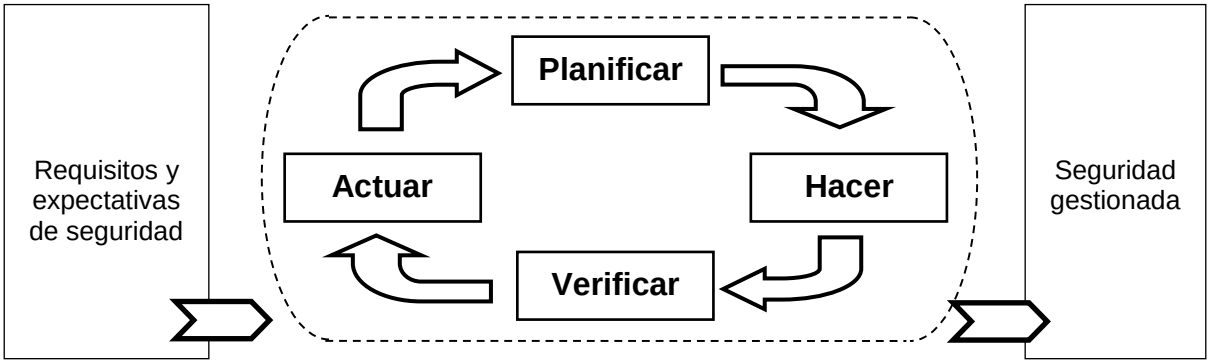
Los tres primeros aspectos son imprescindibles para tomar decisiones efectivas sobre seguridad. Sin un conocimiento razonable de lo que se quiere proteger, contra qué protegerlo y cuan probables son las amenazas, seguir adelante carece de sentido.

La presente metodología promueve la adopción de un enfoque basado en procesos, con el fin de establecer, implementar, operar, dar seguimiento, mantener y mejorar el SGSI de una organización; para ello adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), que se aplica para estructurar todos los procesos del SGSI en correspondencia con la NC-ISO-IEC 27001“Requisitos de los Sistema de Gestión de la Seguridad de la Información” y adecuada a la NC-ISO-IEC 17799 (27002) “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”.

Primera Parte: Sistema de Gestión de la Seguridad Informática

Procesos de un Sistema de Gestión de la Seguridad Informática

El SGSI se compone de cuatro procesos básicos:



Modelo PHVA aplicado a los procesos del SGSI

Planificar (Establecer el SGSI)	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de entregar resultados acordes con las políticas y objetivos globales de la organización.
Hacer (Implementar y operar el SGSI)	Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y su correcta aplicación.
Verificar (Revisar y dar seguimiento al SGSI)	Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (Mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI.

1. Proceso de Planificación del SGSI

Objetivo principal: La realización del análisis y evaluación de los riesgos de seguridad y la selección de controles adecuados.

En esta primera etapa se crean las condiciones para la realización del diseño, implementación y gestión del Sistema de Seguridad Informática, para lo cual se realiza un estudio de la situación del sistema informático desde el punto de vista de la seguridad, con el fin de determinar las acciones que se ejecutan en función de las necesidades detectadas y con ello establecer las políticas, los objetivos, procesos y procedimientos de seguridad apropiados para gestionar el riesgo y mejorar la seguridad informática, lo cual posibilita obtener resultados conformes con las políticas y objetivos globales de la organización.

Los bienes informáticos de que dispone una entidad no tienen el mismo valor, e igualmente, no están sometidos a los mismos riesgos, por lo que es imprescindible la realización de un análisis de riesgos que ofrezca una valoración de los bienes informáticos y las amenazas a las que están expuestos, así como una definición de la manera en que se gestionan dichos riesgos para reducirlos.

Como resultado, se establecen las prioridades en las tareas a realizar para minimizar los riesgos, puesto que estos nunca desaparecen totalmente. La dirección de la entidad asume el riesgo residual, o sea, el nivel restante de riesgo después de su tratamiento.

1.1 Preparación

Durante la preparación se crean las condiciones para el diseño e implementación del SGSI, y se consideran los aspectos siguientes:

1. Asegurar el compromiso de la dirección.
2. Seleccionar y preparar a los miembros del equipo que participa en el diseño e implementación del SGSI.
3. Recopilar información de seguridad.

1.1.1. Compromiso de la dirección de la entidad con la Seguridad Informática

La dirección apoya activamente la seguridad dentro de la organización mediante una orientación clara, compromiso demostrado y la asignación explícita de las responsabilidades de seguridad informática y su reconocimiento, para lo cual:

a) Asegura que los objetivos de seguridad informática estén identificados, cumplan los requisitos de la organización y están integrados en los procesos principales;
b) formula, revisa y aprueba las políticas de seguridad informática;
c) revisa la efectividad de la implementación de las políticas de seguridad;
d) provee una orientación clara y apoyo visible hacia las iniciativas de seguridad;
e) proporciona los recursos necesarios para la seguridad;
f) aprueba la asignación de los roles específicos y responsabilidades en seguridad informática en la organización;
g) inicia planes y programas para mantener la concienciación en seguridad; y
h) asegura que la implementación de los controles de seguridad informática sea coordinada en toda la organización.

1.1.2. Seleccionar y preparar a los miembros del equipo que participan en el diseño e implementación del SGSI

El proceso de diseño e implementación del SGSI no se realiza por una sola persona o por un grupo de personas de una misma especialidad, sino que es el resultado de un trabajo multidisciplinario en el que participen todos aquellos que de manera integral puedan garantizar el cumplimiento de los objetivos planteados.

El equipo de diseño e implementación se conforma con:

1. Directivos y funcionarios que, a los diferentes niveles, responden por la información que se procesa en las tecnologías y por tanto son los garantes de su protección.
2. Personal de informática que domina los aspectos técnicos necesarios para la implementación de los controles de seguridad.
3. Profesionales de la protección, a partir de su responsabilidad en la custodia de los bienes informáticos y otros que se consideren de acuerdo con su perfil.

1.1.3. Recopilar información de seguridad

Durante el proceso de preparación se reúne toda la información que facilite el diseño e implementación del SGSI, para lo que se utilizan los documentos normativos y metodológicos que existan sobre el tema; documentación de aplicaciones y sistemas en explotación en la organización; documentación de incidentes ocurridos en la entidad o en otras organizaciones afines; tendencias de seguridad nacionales e internacionales, así como otros materiales que faciliten su realización.

1.2. Determinación de las necesidades de protección

Las necesidades de protección del sistema informático se establecen mediante la realización de un análisis de riesgos, que es el proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.

La realización del análisis de riesgos proporciona:

a) Una detallada caracterización del sistema informático objeto de protección;
b) la creación de un inventario de bienes informáticos a proteger;
c) la evaluación de los bienes informáticos a proteger en orden de su importancia para la organización;
d) la identificación y evaluación de amenazas y vulnerabilidades;
e) la estimación de la relación importancia-riesgo asociada a cada bien informático (peso de riesgo).

En el proceso de análisis de riesgos se pueden diferenciar dos aspectos:

1. La **Evaluación de Riesgos** orientada a determinar los sistemas que, en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, valoran los riesgos y establecen sus niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la entidad; consiste en el proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar su importancia.
2. La **Gestión de Riesgos** que implica la identificación, selección, aprobación y manejo de los controles a establecer para eliminar o reducir los riesgos evaluados a niveles aceptables, con acciones destinadas a:
   a) Reducir la probabilidad de que una amenaza ocurra;
   b) limitar el impacto de una amenaza, si esta se manifiesta;
   c) reducir o eliminar una vulnerabilidad existente; y
   d) permitir la recuperación del impacto o su transferencia a terceros.

La gestión de riesgos implica la clasificación de las alternativas para manejar los riesgos a que puede estar sometido un bien informático dentro de los procesos en una entidad; implica una estructura bien definida, con controles adecuados y su conducción mediante acciones factibles y efectivas. Para ello se cuenta con las técnicas de manejo del riesgo siguientes:

1. **Evitar:** impedir el riesgo con cambios significativos en los procesos por mejoramiento, rediseño o eliminación, y es el resultado de adecuados controles y acciones realizadas.
2. **Reducir:** cuando el riesgo no puede evitarse por dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible; esta opción es la más económica y sencilla y se consigue con la optimización de los procedimientos y con la implementación de controles.
3. **Retener:** cuando se reduce el impacto de los riesgos pueden aparecer riesgos residuales; dentro de las estrategias de gestión de riesgos de la entidad se plantea como manejarlos para mantenerlos en un nivel mínimo.
4. **Transferir:** es buscar un respaldo contractual para compartir el riesgo con otras entidades, por ejemplo alojamiento, hospedaje, externalización de servicios, entre otros; esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar este.

La necesidad de la actualización permanente del análisis de riesgos está determinada por las circunstancias siguientes:

a) Los elementos que componen un sistema informático en una entidad están sometidos a constantes variaciones: cambios de personal, nuevos locales, nuevas tecnologías, nuevas aplicaciones, reestructuración de entidades, nuevos servicios y otros;
b) la aparición de nuevas amenazas o la variación de la probabilidad de ocurrencia de alguna de las existentes; y
c) pueden aparecer nuevas vulnerabilidades o variar o incluso desaparecer alguna de las existentes, y originan, modifican o eliminan posibles amenazas.

En resumen, durante la determinación de las necesidades de protección del sistema informático es necesario:

1. Caracterizar el sistema informático.
2. Identificar las amenazas potenciales y estimar los riesgos sobre los bienes informáticos.
3. Evaluar el estado actual de la seguridad.

1.2.1 Caracterización del sistema informático

Para el diseño e implementación de cualquier sistema es imprescindible el conocimiento pleno del objeto sobre el cual se quiere diseñar o implantar. Para ello lo más apropiado es precisar los elementos que permitan identificar sus especificidades.

La caracterización del sistema informático incluye la determinación de los bienes informáticos que requieren ser protegidos, su valoración y clasificación según su importancia.

Se precisan los datos que permitan determinar cómo fluye la información entre los diferentes elementos de la entidad, así como entre la entidad y otras instituciones; se considera el carácter de la información y su nivel de clasificación de acuerdo con lo establecido en el país.

Durante la caracterización del sistema informático es necesario establecer además las características de las edificaciones y locales donde están instalados los equipos, tipo de construcción y estructura, lugares o puntos de acceso (ventanas y puertas), visibilidad desde el exterior, ubicación de las TIC, tipos de tecnologías, software instalado, nivel de clasificación de la información que se procesa, documentación de software, preparación y conocimiento del personal que opera los equipos, cualquier otro aspecto que haga más precisa su descripción.

Una buena caracterización del sistema informático permite conocerlo a plenitud y evita pérdida de tiempo e imprecisiones.

Una posible agrupación por categorías que puede ayudar a la identificación de los bienes informáticos a proteger, podría ser la siguiente:

1. **Hardware:** redes de diferente tipo, servidores y estaciones de trabajo, computadoras personales (incluyen portátiles), soportes magnéticos, ópticos y removibles, líneas de comunicaciones, módems, ruteadores, concentradores, entre otros.
2. **Software:** programas fuentes, programas ejecutables, programas de diagnóstico, programas utilitarios, sistemas operativos, programas de comunicaciones, entre otros.
3. **Datos:** generados durante la ejecución, almacenados en discos, información de respaldo, bases de datos, trazas de auditoría, en tránsito por los medios de comunicaciones, entre otros.
4. **Personas:** usuarios, operadores, programadores, personal de mantenimiento, entre otros.
5. **Documentación:** de programas, de sistemas, de hardware, de procedimientos de administración, entre otros.

Una vez identificados los bienes informáticos que necesitan ser protegidos, se determina su importancia dentro del sistema informático y se clasifican según esta.

La valoración de los bienes informáticos posibilita mediante su categorización, determinar en qué medida uno es más importante que otro (grado de importancia) y se toman en cuenta aspectos tales como: la función que realizan, su costo, la repercusión que ocasionaría la pérdida y posibilidad de su recuperación; así como la preservación de la confidencialidad, la integridad y la disponibilidad.

Al estimar la repercusión que ocasiona la pérdida de un bien informático se tiene en cuenta el tiempo que la entidad puede seguir el trabajo sin este, lo que puede ser vital para su funcionamiento. Este tiempo puede oscilar entre escasas horas, hasta días y semanas. Por ejemplo: una agencia bancaria no puede prescindir de su Plan de Cuentas por un número considerable de horas, porque sería imposible su funcionamiento.

Se da el caso que un bien informático puede estar hasta tres semanas dañado. Esto depende de su ciclo de utilización, por ejemplo: si la nómina de una entidad se daña días antes del pago a los trabajadores pondría a la entidad en un serio aprieto, si se dañó después del cobro, habría más tiempo para su recuperación.

La determinación de la importancia de cada bien informático puede ser realizada de forma descriptiva (por ejemplo, valor alto, medio, bajo) o de forma numérica asignan valores entre cero y diez (0 si tiene poca importancia y 10 sí es máxima).

Un resultado inmediato de la caracterización del sistema informático es la conformación de un listado que contenga la relación de los bienes informáticos identificados y clasificados según su importancia.

Bienes informáticos críticos

Como resultado de la evaluación anterior se determinan los bienes informáticos críticos para la gestión de la entidad en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo a que están sometidos. Se consideran bienes informáticos críticos aquellos sin los cuales el trabajo de la entidad no tuviera sentido o no puede ser ejecutado. Por ejemplo:

a) El servidor principal de una red;
b) los medios de comunicaciones de un centro de cobros y pagos remoto;
c) el sistema de control de tráfico aéreo de un aeropuerto;
d) el sistema contable de una entidad.

Los bienes informáticos críticos tienen carácter relativo según la entidad de que se trate, por ejemplo: la destrucción o modificación de una base de datos en una escuela secundaria probablemente no tenga la misma connotación que si ocurre en un centro de investigaciones científicas.

Un aspecto de vital importancia es la concatenación, o sea, la dependencia entre un bien informático y otro. En la práctica se da el caso que un bien informático resulta no ser importante tratado individualmente, para el correcto funcionamiento de una tarea cualquiera, pero como elemento de un sistema, es el preámbulo o paso anterior obligado para el funcionamiento de otro bien informático que ha sido marcado como importante. En este caso todos los activos que cumplen con esa condición han de ser considerados como importantes.

Por otra parte, puede que un recurso sea muy costoso y por ello considerado de importancia alta, y sin embargo no es imprescindible para la gestión de la entidad. Estas circunstancias pueden elevar de forma artificial el nivel de importancia con que ha sido catalogado.

El equipo de trabajo controla que las distintas estructuras que conforman la entidad no declaren importantes aquellos bienes informáticos que en realidad no lo son. Esto evitaría gastos innecesarios. Existe la tendencia de declarar como importantes (críticos) a bienes informáticos que en realidad no lo son. A la hora de tratar este aspecto el equipo de trabajo es lo suficientemente paciente y persuasivo para evitar esta perjudicial práctica.

Lo anterior implica un análisis complementario de los datos obtenidos en el listado de bienes informáticos, que se realiza de la forma siguiente:

1. Señale adecuadamente aquellos bienes informáticos que fueron valorados de importancia significativa.
2. Señale aquellos bienes informáticos, que no han sido valorados de importancia significativa, y tienen una incidencia directa con algún otro bien informático crítico.
3. Señale después de un estudio riguroso y detallado, aquellos bienes informáticos que no tienen una valoración significativa, ni incidencia directa en el trabajo de bienes informáticos críticos, y resulta necesario que sean marcados como tales, por razones prácticas.
4. Ordene el listado de bienes informáticos a partir de las consideraciones anteriores.

1.2.2. Identificación de las amenazas sobre el sistema informático

Una vez que los bienes informáticos que requieren protección son identificados y valorados según su importancia, es necesario identificar las amenazas sobre éstos y estimar el daño (impacto) que puede producir su materialización.

Para cada bien informático a proteger los objetivos fundamentales de seguridad son la confidencialidad, la integridad y la disponibilidad, por lo que hay que determinar cada amenaza sobre la base de como pueda afectar a estas características de la información. El peso que cada una de estas características tiene para los bienes informáticos varía de una entidad a otra, en dependencia de la naturaleza de los procesos informáticos que se llevan a cabo en función de su objeto social. Algunas de las amenazas más comunes son las siguientes:

a) pérdida de información;
b) corrupción o modificación de información;
c) sustracción, alteración o pérdida de equipos o componentes;
d) divulgación de información; e
e) interrupción de servicios.

La realización de un análisis de riesgos implica el examen de cada una de las amenazas sobre los bienes informáticos y su clasificación por niveles, a partir de la probabilidad de su ocurrencia y la severidad del impacto que puedan producir.

1.2.3. Estimación del riesgo sobre los bienes informáticos

La estimación del riesgo sobre cada bien informático se determina con la consideración de las probabilidades de materialización de las amenazas que actúan sobre este. Esto puede ser realizado de forma descriptiva (por ejemplo: riesgo alto, medio, bajo) o de forma numérica asignan valores entre cero y uno (0 sí la probabilidad de que se materialice la amenaza es nula y 1 si es máxima).

Una amenaza puede incidir sobre varios bienes informáticos con la misma probabilidad y sin embargo sus consecuencias no necesariamente son iguales, dependen en cada caso de la importancia del bien de que se trate. La interrelación entre la probabilidad de materialización de las amenazas que actúan sobre un bien informático y la importancia estimada de este, determinan el peso del riesgo. De esta manera se puede determinar el peso del riesgo para cada bien informático.

La evaluación de los riesgos posibilita conocer que bienes informáticos, o que áreas en particular están sometidas a un mayor peso de riesgo y su naturaleza, lo que permite la selección adecuada de los controles de seguridad que son establecidos en cada uno de los casos, y se garantiza de esta manera una correcta proporcionalidad por medio de una adecuada relación entre costos y beneficios.

Es necesario precisar de una manera exhaustiva los riesgos a que está sometido el sistema en cada una de sus partes componentes, a partir de lo cual se pueden determinar con racionalidad los controles de seguridad que son implementados.

La aplicación de los elementos aquí expuestos puede ser realizada con mayor o menor rigor, en dependencia de la composición y preparación del equipo de trabajo designado para acometer esta tarea y de la participación que se dé a otras personas, que sin formar parte del equipo, puedan brindar los elementos que se requiera.

Por otra parte, desde el momento que los resultados dependen de valores estimados, las conclusiones a que se arribe son tomadas como una aproximación al problema, que puede ser ajustada en sucesivas versiones, en correspondencia con la práctica diaria. Los conceptos anteriormente expresados pueden ser aplicados en diversas variantes, pero de alguna forma es imprescindible utilizarlos.

1.2.4. Evaluación del estado actual de la Seguridad Informática

Generalmente las entidades que emplean las TIC en el desarrollo de su actividad, aunque no hayan diseñado un sistema de seguridad informática que considere de forma integral todos los factores a tener en cuenta, tienen implementadas determinadas normas, medidas y procedimientos de seguridad, generalmente de forma empírica a partir de incidentes que han ocurrido o de las experiencias de otras entidades, lo que es insuficiente y da lugar a la existencia de vulnerabilidades.

Es necesario evaluar de manera crítica la efectividad de los controles existentes, sobre la base de los resultados del análisis de riesgos realizado, con el objetivo de perfeccionarlos o sustituirlos por aquellos que brinden la respuesta adecuada. Los resultados de esta evaluación ayudan a orientar y a determinar una apropiada acción gerencial y las prioridades para gestionar los riesgos de seguridad informática, así como la implementación de los controles seleccionados para protegerse.

La determinación de las necesidades de protección examinada en este apartado da como resultado la definición de los aspectos principales siguientes:

1. Cuáles son los bienes informáticos más importantes a proteger.
2. Que amenazas tienen mayor probabilidad de actuar sobre los bienes informáticos y su posible impacto sobre la entidad.
3. Que áreas están sometidos a un mayor peso de riesgo y que amenazas los motivan.
4. Que controles de seguridad son perfeccionados o sustituidos y en qué caso se requiere definir e implementar alguno nuevo.

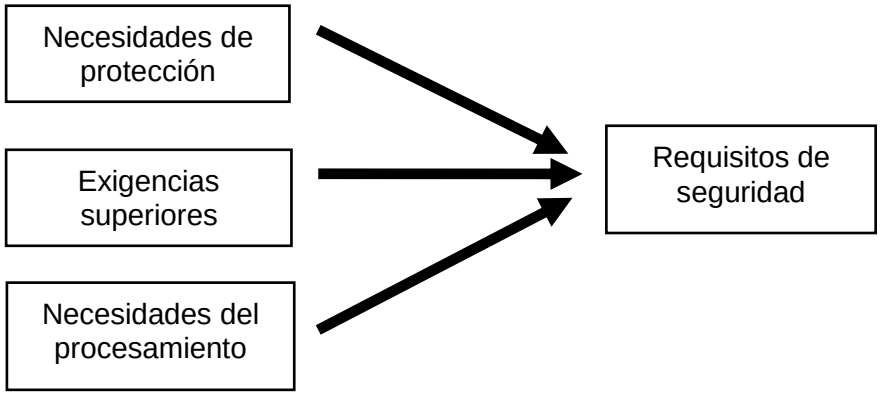
Llegado a este punto es necesario:

1. Identificar y evaluar alternativas posibles para tratar los riesgos.
2. Seleccionar e implantar los controles que permitan reducir el riesgo a un nivel aceptable.
3. Identificar los riesgos residuales que han quedado sin cubrir.
4. Preparar un plan para el tratamiento de los riesgos.
5. Preparar procedimientos para implantar los controles.

1.3 Establecimiento de los requisitos de Seguridad Informática

Parte esencial del proceso de planificación consiste en la identificación de los requisitos de seguridad de la organización. Existen tres fuentes principales:

1. La determinación de las necesidades de protección de la organización, durante la cual se identifican los bienes informáticos más importantes; las amenazas a que están sometidos; se evalúa la vulnerabilidad y la probabilidad de ocurrencia de las amenazas y se estima su posible impacto.
2. El conjunto de requisitos instituidos por obligaciones contractuales, normas legales y técnicas que satisfacen la organización.
3. Los principios, objetivos y requisitos que forman parte del procesamiento de la información que la organización ha desarrollado para apoyar sus operaciones.



Los requisitos de seguridad se identifican mediante la evaluación de los riesgos. El gasto en controles se equilibra con el perjuicio para la organización resultante de los fallos de seguridad (costo-beneficio).

1.4 Selección de los controles de Seguridad Informática

Antes de considerar el tratamiento de los riesgos, la organización decide los criterios para determinar si pueden ser aceptados o no. Un riesgo puede ser aceptado si, por ejemplo, se determina que es bajo o que el costo de su tratamiento no es rentable para la organización.

Para cada uno de los riesgos identificados se toma una decisión sobre su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

a) **Aplicar controles apropiados** para reducir los riesgos;
b) **Aceptar riesgos** de manera consciente y objetiva, siempre que satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos;
c) **Evitar riesgos**, no permitir las acciones que propicien los riesgos;
d) **Transferir los riesgos** a otras partes, por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde se decida aplicar controles apropiados, se seleccionan e implantan para lograr los requisitos identificados mediante la evaluación de riesgos. Los controles aseguran que estos son reducidos a un nivel aceptable y se toman en cuenta:

a) requisitos y restricciones de la legislación y de las regulaciones nacionales e internacionales;
b) objetivos de la organización;
c) requisitos y restricciones operacionales;
d) costo de la implementación y de la operación;
e) la necesidad de balancear la inversión en la implementación y la operación de controles contra el daño probable como resultado de fallas de la seguridad.

Los controles de seguridad que se seleccionen para la reducción de los riesgos a un nivel aceptable cubren adecuadamente las necesidades específicas de la organización. La selección de los controles de seguridad depende de una decisión organizacional basada en los criterios para la aceptación del riesgo, las opciones para su tratamiento, y el acercamiento a su gestión general aplicada a la organización, y también está conforme con toda la legislación y regulaciones nacionales e internacionales vigentes.

Los objetivos de control y los controles se basan en: los resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo; en los requisitos legales o reglamentarios; en las obligaciones contractuales y en las necesidades orgánicas de la entidad en materia de seguridad informática.

Los controles de seguridad informática son considerados en las etapas de especificación de requisitos y de diseño de sistemas y aplicaciones. El no hacerlo puede dar lugar a costos adicionales y a soluciones menos eficaces, y en el peor de los casos, imposibilidad de alcanzar la seguridad adecuada. Estos controles son establecidos, implementados, supervisados y mejorados cuando sea necesario para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

Hay que tener presente que ningún sistema de controles puede alcanzar la seguridad completa y que acciones adicionales de gestión se implementan para supervisar, evaluar, y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la organización.

La seguridad informática se logra implantar con un conjunto adecuado de controles, que incluyen políticas, procesos, medidas, procedimientos, estructuras organizativas y funciones de hardware y software. Nos referiremos a continuación específicamente a las políticas y a las medidas y procedimientos de seguridad informática.

1.4.1. Políticas de Seguridad Informática

El objetivo fundamental de la definición de las Políticas de Seguridad Informática consiste en proporcionar orientación y apoyo de la dirección para la seguridad informática, de acuerdo con los requisitos de la organización y con las regulaciones y leyes vigentes.

La dirección establece políticas de seguridad en correspondencia con los objetivos de la entidad y demuestra su apoyo y compromiso a la seguridad informática, con la publicación y el mantenimiento de esas políticas en toda la organización, las cuales se comunican a todos los usuarios de manera apropiada, accesible y comprensible.

Las políticas de seguridad definen los "QUE": **qué** debe ser protegido, **qué** es más importante, **qué** es más prioritario, **qué** está permitido y **qué** no lo está y **qué** tratamiento se le dan a los problemas de seguridad. Las políticas de seguridad en sí mismas no dicen "COMO" las cosas son protegidas. Esto es función de las medidas y procedimientos de seguridad.

Las políticas de seguridad conforman la estrategia general. Las medidas y procedimientos establecen en detalle los pasos requeridos para proteger el sistema informático. No puede haber medidas y procedimientos que no respondan a una política, al igual que no puede concebirse una política que no esté complementada con las medidas y procedimientos que le correspondan.

Comenzar con la definición de las políticas de seguridad a partir de los riesgos estimados asegura que las medidas y procedimientos proporcionen un adecuado nivel de protección para todos los bienes informáticos.

Desde que las políticas de seguridad pueden afectar a todo el personal en una entidad es conveniente asegurar tener el nivel de autoridad requerido para su establecimiento. La creación de las políticas de seguridad es avalada por la máxima dirección de la organización que tiene el poder de hacerlas cumplir. Una política que no se puede implementar y hacer cumplir es inútil.

Uno de los objetivos básicos al desarrollar las políticas de seguridad consiste en definir qué se considera uso apropiado de los sistemas informáticos; así como la forma en que se tratan los incidentes de seguridad. Para esto son considerados los criterios siguientes:

1. Tener en cuenta el objeto social de la entidad y sus características. Por ejemplo la seguridad de una entidad comercial es muy diferente a la de un organismo central o a la de una universidad.
2. Las políticas de seguridad que se desarrollen están en correspondencia con las políticas, reglas, regulaciones y leyes a las que la entidad está sujeta.
3. A menos que el sistema informático a proteger esté completamente aislado e independiente, hay que considerar las implicaciones de seguridad en un contexto más amplio. Las políticas manejan los asuntos derivados de un problema de seguridad que tiene lugar por causa de un sitio remoto, así como un problema que ocurre en este como resultado de un usuario o computadora local.

Algunas de las interrogantes que se resuelven al diseñar una política de seguridad son las siguientes:

1. ¿Qué estrategia se adopta para la gestión de la seguridad informática?
2. ¿A quién se le permite utilizar los bienes informáticos?
3. ¿Qué se entiende por uso correcto de los recursos?
4. ¿Quién está autorizado para garantizar el acceso y aprobar el uso de los bienes informáticos?
5. ¿Quién tiene privilegios de administración de los sistemas?
6. ¿Cuáles son los derechos y responsabilidades de los usuarios?
7. ¿Cuáles son los derechos y responsabilidades de los administradores de sistemas frente a los de los usuarios?
8. ¿Qué hacer con la información clasificada y limitada?
9. ¿Qué hacer ante la ocurrencia de un incidente de seguridad?

Estas no son las únicas interrogantes que son resueltas en el diseño de las políticas. En la práctica surgen otras no menos importantes.

Las principales características que tiene una buena política de seguridad son:

1. Poder implementarse a través de medidas y procedimientos, la publicación de principios de uso aceptable u otros métodos apropiados.
2. Poder hacerse cumplir por medio de herramientas de seguridad, donde sea apropiado y con sanciones, donde su prevención no sea técnicamente posible.
3. Definir claramente las áreas de responsabilidad de los usuarios, administradores y directivos.

Entre los componentes que forman parte de las políticas de seguridad se incluyen:

a) el tratamiento que requiere la información oficial que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, según su categoría;
b) el empleo conveniente y seguro de las tecnologías instaladas y cada uno de los servicios que éstas pueden ofrecer;
c) la definición de los privilegios y derechos de acceso a los bienes informáticos para garantizar su protección contra modificaciones no autorizadas, pérdidas o revelación, mediante la especificación de las facultades y obligaciones de los usuarios, especialistas y directivos;
d) los aspectos relacionados con la conexión a redes de alcance global y la utilización de sus servicios;
e) el establecimiento de los principios que garanticen un efectivo control de acceso a las tecnologías (incluyen el acceso remoto) y a los locales donde éstas se encuentren;
f) las normas generales relacionadas con la información de respaldo y su conservación;
g) los principios a tener en cuenta sobre los requerimientos de Seguridad Informática que deben ser considerados en la adquisición de nuevas tecnologías;
h) los aspectos relacionados con la adquisición por cualquier vía de software y documentos de fuentes externas a la entidad y la conducta a seguir en estos casos;
i) la definición de las responsabilidades de los usuarios, especialistas y directivos, sus derechos y obligaciones con respecto a la Seguridad Informática;

j) la definición de los principios relacionados con el monitoreo del correo electrónico, la gestión de las trazas de auditoría y el acceso a los ficheros de usuario, entre otros;
k) las normas a tener en cuenta en relación con el mantenimiento, reparación y traslado de las tecnologías y del personal técnico (interno y externo) que requiere del acceso a estas por esos motivos;
l) los principios generales para el tratamiento de incidentes y violaciones de seguridad, qué se considera incidente de seguridad y a quién reportar.

Las políticas de seguridad informática son revisadas a intervalos programados o ante el surgimiento de cambios significativos para asegurar su actualización, adecuación y efectividad.

A continuación se muestran dos ejemplos de políticas:

1. El acceso a las áreas o zonas controladas se permite exclusivamente al personal autorizado.
2. El acceso a los medios informáticos es expresamente autorizado por el jefe facultado.

Obsérvese que en el primer ejemplo la política expresada limita explícitamente al personal autorizado el acceso a las áreas o zonas controladas, pero no especifica cuáles son las áreas o zonas definidas como controladas, cómo se garantiza el control en cada una de ellas, que personal es autorizado, quién está facultado para otorgar las autorizaciones, cuando se requieren estas autorizaciones y qué forma tiene la autorización (por escrito, verbal, etc.). Es aplicable en todas las áreas controladas de la entidad independientemente de su categoría (limitada, restringida o estratégica) y de la forma de su implementación en cada caso.

De igual manera en el segundo ejemplo, no se menciona cómo se realiza la autorización de los usuarios para acceder a los medios informáticos, cuando se efectúe, ni quién es la persona facultada para hacerlo. Todas esas “aparentes insuficiencias” corresponden ser despejadas con medidas y procedimientos ajustados a las características propias de cada lugar donde corresponda aplicar esas políticas, que por supuesto no tienen por qué ser iguales en cada caso. Por ello las medidas y procedimientos sí tienen que especificar en detalle lo que hay que hacer, pues al contrario de las políticas que están destinadas para toda la entidad, son específicas en función de las necesidades de cada área.

De lo anterior se infiere que cualquier política que se establezca necesita ser instrumentada mediante las medidas y procedimientos que garanticen su cumplimiento en cada área que lo necesite y viceversa. Debido a esto, se requiere contrastar las medidas y procedimientos que se implanten con las políticas definidas para comprobar que no existan unas sin respaldo de las otras.

1.4.2. Medidas y procedimientos de Seguridad Informática

Las medidas y procedimientos de seguridad que se implementen en correspondencia con las políticas definidas, conforman el cuerpo del sistema de seguridad diseñado y representan la línea de defensa básica de protección de los bienes informáticos, por lo que es sumamente importante su selección adecuada, de forma tal que cubran las amenazas identificadas durante el proceso de evaluación de riesgos, y se implementen de una manera rentable.

Si la mayor amenaza al sistema es un acceso remoto, tal vez no tenga mucha utilidad el empleo de dispositivos técnicos de control de acceso para usuarios locales. Por otro lado si la mayor amenaza es el uso no autorizado de los bienes informáticos por los usuarios habituales del sistema, probablemente es necesario establecer rigurosos procedimientos de monitoreo y de gestión de auditoría.

Las medidas y procedimientos que se establecen son definidos de manera suficientemente clara y precisa, para evitar interpretaciones ambiguas por parte de los responsabilizados con su cumplimiento.

La seguridad es implementada mediante el establecimiento de múltiples barreras de protección, la selección de controles de diferentes tipos de forma combinada y concéntrica, para lograr con ello una determinada redundancia que garantice que si una medida falla o resulta vulnerada, la siguiente medida entre en acción y continúe la protección del activo o recurso. No es conveniente que el fallo de un solo mecanismo comprometa totalmente la seguridad.

La implementación de múltiples medidas simples puede en muchos casos ser más seguro que el empleo de una medida muy sofisticada. Esto cobra mayor validez cuando determinada medida no puede ser aplicada por alguna limitación existente, como pueden ser, por ejemplo: las insuficiencias del equipamiento, que impiden la implementación de una medida técnica. En este caso son consideradas medidas o procedimientos complementarios de otro tipo, que garanticen un nivel de seguridad adecuado.

Hay que tener en cuenta también que el uso del sentido común y una buena gestión son las herramientas de seguridad más apropiadas. De nada vale diseñar un sistema de medidas muy complejo y costoso si se pasan por alto los controles más elementales. Por ejemplo, independientemente de cuán sofisticado sea un sistema de control de acceso, un simple usuario con una clave pobre o descuidada puede abrir las puertas del sistema.

Otro elemento importante a considerar al implementar las medidas y procedimientos es aplicar el principio de proporcionalidad o racionalidad, que consiste en ajustar su magnitud al riesgo presente en cada caso. Por ejemplo, la salva de la información puede tener diferentes requerimientos en distintas áreas y en una misma área para distintos tipos de datos o programas.

Las medidas de Seguridad Informática se clasifican de acuerdo con su origen en: administrativas; de seguridad física, técnica o lógica; de seguridad de operaciones; legales y educativas. A su vez, por su forma de actuar, las medidas pueden ser: preventivas, de detección y de recuperación.

Medidas administrativas

Las medidas administrativas, frecuentemente no son apreciadas en toda su importancia, a pesar de que la práctica ha demostrado que un elevado por ciento de los problemas de seguridad se puede evitar con medidas de esta naturaleza.

Se establecen por la dirección de cada entidad mediante las regulaciones comprendidas dentro de sus facultades y por tanto, son de obligatorio cumplimiento por todo el personal hacia el cual están dirigidas.

Medidas de seguridad física

Constituyen la primera barrera de protección en un Sistema de Seguridad Informática e introducen un retardo que incrementa el tiempo de materialización de un acto doloso o accidental.

Se aplican a los locales donde se encuentran las tecnologías de información y directamente a estas mismas tecnologías e incluyen: medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.

Medidas técnicas o lógicas

Son las de mayor peso dentro de un sistema de Seguridad Informática. Pueden ser implementadas por software, a nivel de sistemas operativos y de aplicaciones o por hardware. El uso combinado de técnicas de software y hardware aumenta la calidad y efectividad en la implementación de este tipo de medidas.

Algunos tipos de medidas técnicas son empleadas para identificar y autentificar usuarios, protección criptográfica, protección contra virus y otros programas dañinos y registro de auditoría, entre otros.

Medidas de seguridad de operaciones

Están dirigidas a lograr una eficiente gestión de la seguridad mediante la ejecución de procedimientos definidos y garantizan el cumplimiento de las regulaciones establecidas por cada entidad y por las instancias superiores a esta.

Medidas legales

Representan un importante mecanismo de disuasión que contribuye a prevenir incidentes de seguridad y sancionar adecuadamente a los violadores de las políticas establecidas por la entidad.

Se establecen mediante disposiciones jurídicas y administrativas, en las que se plasman: deberes, derechos, funciones, atribuciones y obligaciones, así como se tipifican las violaciones y tipos de responsabilidad administrativas, civiles, penales u otras.

Medidas educativas

Están dirigidas a inculcar una forma mental de actuar, mediante la cual el individuo esté consciente de la existencia de un Sistema de Gestión de la Seguridad Informática en el que le corresponde una forma de actuar. Se sustentan en dos elementos fundamentales:

1. La existencia de un Sistema de Gestión de la Seguridad Informática.
2. La participación consciente del hombre en el éxito de los objetivos de seguridad planteados.

Medidas de recuperación

Están dirigidas a garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos ante cualquier eventualidad que pueda ocurrir, que afecte o ponga en peligro su normal desarrollo.

Se establecen a partir de la identificación de los posibles incidentes o fallas que puedan causar la interrupción o afectación de los procesos informáticos y garantizan las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios para ello.

Procedimientos de Seguridad Informática

La implementación de las políticas de seguridad informática requiere generalmente la realización de un conjunto de acciones para garantizar su cumplimiento. La descripción de esta secuencia de acciones constituye un procedimiento de seguridad. Los procedimientos, al igual que las medidas, se clasifican en procedimientos de prevención, de detección y de recuperación.

Los **procedimientos de prevención** tienen el objetivo de asegurar las acciones que se requieren para evitar que una amenaza se materialice y los **de detección** se dirigen a identificar cualquier tipo de indicio que revele la posible materialización de una amenaza, una amenaza en desarrollo o una vulnerabilidad en los sistemas.

La función de los **procedimientos de recuperación**, por el contrario, no es la de prevenir ni la de detectar la materialización de determinadas amenazas, sino la de establecer las acciones que se ejecutan cuando una amenaza ya se ha materializado y afectan parcial o totalmente los bienes informáticos.

En el desarrollo de los procedimientos se usa un lenguaje preciso y una cuidadosa redacción y quedan claras las ideas principales, de forma tal que resulten comprensibles a quienes corresponda su aplicación. Los procedimientos son autosuficientes.

La importancia del establecimiento de procedimientos correctamente definidos garantiza, además de la uniformidad en la aplicación de las políticas, la seguridad de su cumplimiento y su sistematicidad. Algunos procedimientos de seguridad que pueden ser implementados son:

a) De administración de cuentas de usuarios;
b) de asignación y cancelación de permisos de acceso a las tecnologías y sus servicios;
c) de asignación y cancelación de derechos y privilegios;
d) de gestión de incidentes;
e) de gestión de contraseñas;
f) de gestión de salvas;
g) de realización de auditorías;
h) de acceso a las áreas;

i) de entrada y salida de las tecnologías y sus soportes.

Ejemplo de una política y de algunas medidas y procedimientos para su implementación.

Política: "La información es salvada en soportes magnéticos u ópticos con la periodicidad requerida en cada caso, a fin de garantizar su restablecimiento en caso de incidentes de seguridad".

Medidas:

1. La información que se comparte en los servidores de la red se salva en los casetes de cinta habilitados al efecto, diariamente en dos versiones.
2. Las bases de datos de contabilidad son salvadas en discos reescribibles en dos versiones. Diariamente se salvan las modificaciones realizadas y mensualmente toda la información.

Procedimientos:

a) En los servidores:

1. Realizar la salva de la información que se comparte en los servidores en dos casetes numerados, se alternan diariamente, una hora antes de concluir la jornada de trabajo. Utilizar el casete marcado con el No. 1 los días impares y con el No. 2 los días pares.
   Responsable: Administrador de la red
2. Anotar en el modelo de registro establecido (anexo N) la fecha, la hora y el casete utilizado.
   Responsable: Administrador de la red
3. Verificar integridad de la información salvada.
   Responsable: Jefe de Departamento de Redes
4. Guardar la salva bajo llave en el archivo metálico ubicado en la oficina del Jefe del Departamento de Redes.
   Responsable: Jefe del Departamento de Redes

b) En el Departamento de Contabilidad:

1. Realizar la salva de las bases de datos en discos compactos, se alternan diariamente, al finalizar la jornada de trabajo y el último día hábil de cada mes. Los discos para la salva diaria están marcados con una franja, se utilizan los de la franja roja para los días impares y los de la franja azul para los días pares. Los discos para la salva mensual son numerados del 1 al 12 en correspondencia con cada mes.
   Responsable: Administrador de la aplicación
2. Anotar en el modelo de registro establecido (anexo M) la fecha, la hora y el disco utilizado.
   Responsable: Administrador de la aplicación
3. Verificar integridad de la información salvada.
   Responsable: Jede de Departamento de Contabilidad
4. Guardar la salva bajo llave en el archivo metálico ubicado en la oficina del Jefe del Departamento de Contabilidad.
   Responsable: Jefe del Departamento de Contabilidad

1.5. Organización de la Seguridad Informática

Con el objetivo de gestionar la seguridad informática se establece un marco apropiado para iniciar y controlar su implementación dentro de la organización.

1.5.1. Organización interna

La dirección aprueba las políticas de seguridad informática de la entidad, asigna roles de seguridad, coordina y revisa la implementación de la seguridad a través de la organización.

Si es necesario, gestiona una fuente de asesoramiento especializada en seguridad informática. Son establecidos contactos con especialistas de seguridad o grupos externos a la organización, incluyen autoridades pertinentes, para mantenerse al día con tendencias de la industria, seguimiento de normas, métodos de evaluación y proveer puntos de enlace adecuados cuando se deban manejar incidentes de seguridad informática. Se propicia un enfoque multidisciplinario hacia la seguridad informática.

1.5.2. Coordinación de la Seguridad Informática

Las actividades referentes a la seguridad informática son coordinadas por los Consejos de Dirección de los órganos, organismos y entidades, que pueden incluir personal de diferentes partes de la organización con funciones y roles específicos. Esta coordinación:

a) asegura que las actividades referentes a la seguridad son ejecutadas de acuerdo a las políticas establecidas;
b) identifica cómo manejar los incumplimientos;
c) aprueba metodologías y procedimientos para la seguridad informática, por ejemplo, de evaluación de riesgos, respaldo de la información y tratamiento de incidentes;
d) identifica cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas;
e) evalúa la adecuación y coordinación de la implementación de los controles de seguridad informática;
f) promueve en forma efectiva la educación, la formación y la concienciación en seguridad informática a través de la organización;
g) evalúa la información resultante del tratamiento y análisis de los incidentes de seguridad informática y las acciones recomendadas en su respuesta.

1.5.3. Asignación de responsabilidades sobre Seguridad Informática

Se definen las responsabilidades de seguridad informática del personal vinculado con el sistema informático de acuerdo con su participación en este. La asignación de las responsabilidades de seguridad informática se hace en correspondencia con las políticas de seguridad informática, se definen claramente las responsabilidades asociadas con la protección de los bienes informáticos y para la

ejecución de procesos específicos de seguridad, como por ejemplo, la gestión de incidentes. Estas responsabilidades son complementadas, de ser necesario, con medidas y procedimientos específicos.

Las personas con responsabilidades de seguridad asignadas pueden delegar tareas de seguridad a otras, sin embargo, mantienen la responsabilidad y garantizan que cualquier tarea delegada se ha cumplido correctamente. Se establecen claramente las áreas de las cuales los individuos son responsables. En particular se considera lo siguiente:

a) definir y documentar los niveles de autorización;
b) identificar y definir los bienes informáticos y los procesos de seguridad asociados con cada sistema específico;
c) asignar el responsable de cada bien informático o proceso de seguridad y documentar los detalles de dicha responsabilidad.

Se asegura que cada cual conozca su responsabilidad en relación con el mantenimiento de la seguridad y que cada clase de problema tenga alguien asignado para tratarlo; y se involucra a todo el personal relacionado con los bienes informáticos. Por ejemplo, los usuarios son responsables del uso adecuado de sus identificadores y contraseñas y los administradores de redes y sistemas están obligados a cubrir las brechas de seguridad y corregir los errores. Para alcanzar una seguridad efectiva es conveniente lograr una participación lo más amplia posible de todo el personal (o al menos la ausencia de una oposición activa).

Se establecen niveles de responsabilidad asociados con las políticas de seguridad. Por ejemplo, en una red se puede definir un nivel con sus usuarios, donde cada uno tiene la responsabilidad de proteger su cuenta. Un usuario que permita que su cuenta sea comprometida incrementa la posibilidad de comprometer otras cuentas o recursos. Los administradores de redes y sistemas forman otro nivel de responsabilidad; se implementan los mecanismos de seguridad que se requieran.

Queda claro que los usuarios son individualmente responsables de la comprensión y aplicación de las políticas de seguridad de los sistemas que ellos emplean y del uso apropiado de los recursos que les han sido asignados.

1.6. Elaboración del Plan de Seguridad Informática

Una vez cumplidas las actividades anteriores, el siguiente paso es la elaboración del Plan de Seguridad Informática, en lo adelante PSI como constancia documentada del Sistema de Seguridad Informática diseñado y constituye el documento básico que recoge claramente las responsabilidades de cada uno de los participantes en el proceso informático y establece los controles que permiten prevenir, detectar y responder a las amenazas que gravitan sobre el sistema informático de cada entidad.

El objetivo del PSI es establecer los requisitos de seguridad del sistema y en él se especifican los controles previstos en cada área o lugar para cumplirlos. El PSI también describe las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema y refleja las contribuciones de los distintos actores con responsabilidades sobre el SGSI.

En el PSI se refiere **cómo** se implementan, en las áreas a proteger, las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, de acuerdo con sus formas de ejecución, periodicidad, personal participante y medios**.**

Se particularizan en el PSI los controles de seguridad implementados en correspondencia con su naturaleza, de acuerdo con el empleo que se haga de los recursos humanos, de los medios técnicos o de las medidas y procedimientos que cumple el personal. **En la Segunda Parte: Estructura y contenido del Plan de Seguridad Informática** se refieren con mayor detalle los elementos necesarios para la elaboración del PSI.

2. Proceso de Implementación del SGSI

Objetivo principal: garantizar una adecuada implementación de los controles seleccionados y su correcta aplicación.

Durante el proceso de implementación del SGSI se comienzan a gestionar los riesgos identificados mediante la aplicación de los controles seleccionados y las acciones apropiadas por parte del personal definido (recursos humanos), los recursos técnicos disponibles en función de la seguridad (medios técnicos) y las medidas administrativas, que garanticen la implantación de controles efectivos para lograr el nivel de seguridad necesario, en correspondencia con los objetivos de la organización, de manera que se mantenga siempre el riesgo por debajo del nivel asumido por la propia entidad.

Se garantiza que el personal al que se asignen responsabilidades definidas en el SGSI esté en capacidad de realizar las tareas exigidas, mediante la formación y el entrenamiento que les permita adquirir el conocimiento y las habilidades que requieran, en correspondencia con su papel dentro del sistema, para lo que se implementan programas de capacitación.

La organización también asegura que el personal tiene conciencia de la necesidad e importancia de las actividades de seguridad informática que le corresponde realizar y cómo ellas contribuyen al logro de los objetivos del SGSI.

Las actividades de formación y sensibilización incluyen:

1. Concienciar al personal de la importancia que el SGSI tiene para la organización.
2. Garantizar la divulgación, el conocimiento y comprensión de las políticas de seguridad que se implementan.
3. Capacitar a los usuarios en las medidas y procedimientos que se van a implantar.
4. Lograr que el personal esté consciente de los roles a cumplir dentro del SGSI.

Se requiere además precisar el procedimiento de medición de la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se van a emplear estas mediciones, con la finalidad de evaluar su eficacia para producir resultados comparables y reproducibles y de esta forma, determinar si las actividades de seguridad implementadas satisfacen las expectativas concebidas.

Finalmente se implementan los procedimientos y controles que se requieran para detectar y dar respuesta oportuna a los incidentes de seguridad que se presenten, que incluyen su reporte a las instancias pertinentes.

El proceso de implementación es una etapa crucial del SGSI y tal vez la más difícil. De nada vale haber realizado una buena determinación de las necesidades de protección e incluso haber hecho una excelente selección de los controles de seguridad a aplicar, si no se logra implantarlos en cada lugar, se ajustan a las particularidades de los bienes a proteger y a las exigencias específicas de cada área.

Se puede haber definido, por ejemplo, una refinada política de respaldo de la información en previsión de cualquier tipo de contingencia que pudiera presentarse, y no implementar los procedimientos que determinen con exactitud qué información es preservada; con qué frecuencia se salva, en qué soporte y en cuantas copias; quienes están encargados de ejecutar esas acciones y como se garantiza su protección y conservación, de manera que exista la certeza de su integridad cuando requieran ser utilizadas.

Puede haberse confeccionado un Plan de Seguridad Informática que cumpla a cabalidad los requisitos metodológicos, pero en sus partes esenciales se queda “en el papel” y no se conoce ni se aplica por los que tienen que instrumentar los controles que fueron definidos. Por ejemplo, en ocasiones se especifica en el plan la estructura y fortaleza de las contraseñas de acceso a la red y sin embargo, no se configuran en el servidor las reglas que en correspondencia con lo establecido obliguen a los usuarios a su cumplimiento.

De igual forma, pueden haberse concebido los procedimientos para otorgar o cancelar el acceso a sistemas y servicios pero estos no se conocen o se incumplen por los que tienen que ejecutarlos regularmente. Ejemplos semejantes pueden referirse en relación con la gestión de parches de seguridad, la seguridad de las redes inalámbricas, el control de los soportes removibles, la gestión de incidentes y el análisis y conservación de los registros generados por los sistemas y servicios, por solo citar algunos de los más comunes.

De modo que el proceso de implementación del SGSI para que sea exitoso garantiza la implantación de todos los controles que fueron concebidos y su conocimiento y comprensión por los encargados de ejecutarlos y cumplirlos.

2.1. Programa de Desarrollo de la Seguridad Informática

Puede ser que la implementación de algunos controles requiera de un tiempo adicional, ya sea porque necesitan algún tipo de recursos con que no se cuenta, la realización de gestiones complementarias u otras causas. Las acciones que sean necesarias para lograr la implementación de estos controles se incluyen en un programa que señala los plazos para su cumplimiento y el personal responsabilizado con su ejecución. Los aseguramientos que se deriven de estas acciones son considerados dentro del Plan de Inversiones de la entidad cuando se requiera. El cumplimiento de este programa contribuye al proceso de mejora continua del SGSI y es actualizado según se ejecute. Algunos aspectos a considerar al elaborar el Programa de Desarrollo de la Seguridad Informática pudieran ser los siguientes:

1. La implementación a mediano y largo plazo de aquellos aspectos que así lo exijan para alcanzar un mayor nivel de seguridad, como por ejemplo la introducción de medios técnicos de seguridad, modificación de locales, etc.
2. La preparación y capacitación del personal en materia de seguridad informática, según su participación en el sistema diseñado, ya sea a través de cursos específicos, mediante la impartición de materias relacionadas con el tema y con acciones de divulgación.
3. La organización y ejecución de controles, inspecciones y auditorías (internas y externas), mencionan con qué frecuencia se realizan, quienes participan y su contenido.

2.2 Factores Críticos de éxito

La implementación exitosa de los controles seleccionados y su correcta aplicación en una organización presupone, además, la consideración de los factores siguientes:

a) La política de seguridad, objetivos y actividades que reflejen los intereses de la organización;
b) el enfoque para implantar la seguridad que sea consistente con la cultura de la organización;
c) el apoyo visible y el compromiso de la alta dirección;
d) la buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo;
e) la comunicación eficaz de la necesidad de la seguridad a todos los directivos y trabajadores;
f) la distribución a todos los trabajadores de directrices y normas sobre la política de seguridad informática de la organización;
g) suministrar recursos para las actividades de gestión de la seguridad informática;
h) proporcionar concienciación, formación y educación apropiadas;
i) proceso efectivo de gestión de incidentes de seguridad informática;
j) implementación de un sistema de medición para evaluar el desempeño en la gestión de seguridad informática y las sugerencias de mejoras.

Durante el proceso de implementación del SGSI es necesario precisar la aplicación de cada uno de los controles seleccionados en las áreas que los requieren y que cubran los riesgos que para ellas fueron identificados. En este sentido, la participación de los jefes de áreas es determinante, pues corresponde a ellos refrendar que los controles que se establezcan dan plena respuesta a los requerimientos de protección de cada área en particular.

Para cumplir con lo expresado en el párrafo anterior se elabora un cronograma de implementación por áreas, mediante el cual los jefes de estas garanticen:

1. La concienciación del personal sobre la necesidad e importancia de sus actividades de Seguridad Informática y cómo ellas contribuyen al logro de los objetivos del SGSI.
2. La preparación del personal para el cumplimiento de sus obligaciones en cuanto a la Seguridad Informática.
3. La implantación de los controles de seguridad, tanto los comunes para toda la entidad como los específicos para el área.
4. La verificación de que los controles aplicados garantizan el cumplimiento de las políticas de seguridad establecidas en la organización.
5. La precisión de los métodos de evaluación de la eficacia de los controles que se implementen.
6. La identificación de los controles que no es posible implantar y deban ser incluidos en el Programa de Desarrollo de la Seguridad Informática.

No se puede dar por terminado el proceso de implementación del SGSI por el dirigente máximo de la entidad, hasta que en todas las áreas sus Jefes acrediten el cumplimiento de estos requisitos.

3. Proceso de Verificación del SGSI

Objetivo principal: Revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
Uno de los aspectos más importantes en el proceso de diseño e implementación de un SGSI es el establecimiento de los indicadores y métricas de gestión. Esto permite a la Dirección valorar si los esfuerzos realizados cumplen o no con los objetivos planteados. Para ello se utiliza la medición como instrumento de control. Es necesario lograr diagnosticar correctamente qué pasa y qué es necesario corregir para poder gestionar.

Mediante el proceso de revisión se comprueba la conformidad con los patrones establecidos y como parte de ello se mide el rendimiento y la eficacia del SGSI, para lo cual se precisa considerar las acciones siguientes:

1. Revisiones periódicas de los indicadores seleccionados.
2. Revisiones de los riesgos residuales y riesgos aceptables.
3. Realización de auditorías internas/externas del SGSI.
4. Comunicación de los resultados de las auditorías a las partes interesadas.

La ejecución de procedimientos de revisión mediante instrumentos de medición posibilita detectar errores de proceso, identificar fallos de seguridad de forma rápida y determinar las acciones a realizar. Se utilizan para ello los indicadores seleccionados sobre la base de los criterios en relación a qué aspectos se controlan y miden para lograr el cumplimiento de las metas planteadas.

Los objetivos de estos procedimientos de revisión son:

1. Evaluar la efectividad de la implementación de los controles de seguridad.

2. Evaluar la eficiencia del SGSI, incluyen mejoras continuas.
3. Proveer estados de seguridad que guíen las revisiones del SGSI, faciliten mejoras a la seguridad y nuevas entradas para auditar.
4. Comunicar valores de seguridad a la organización.
5. Servir como entradas al análisis y tratamiento de riesgos.

La gestión del Sistema de Seguridad Informática se basa en un ciclo de mejora continua, por lo que es vital medir para poder observar cómo las cosas mejoran a medida que el sistema madura. Si no se mide, se trabaja en base a sensaciones, y las decisiones tomadas sin la información necesaria pueden conducir a equivocaciones.
Pasado el tiempo previsto de antemano, hay que volver a recopilar datos de control y analizarlos, compararlos con los objetivos y especificaciones iniciales, para evaluar si se han producido cambios que afecten los resultados esperados. Donde sea aplicable, se mide el desempeño del SGSI contra las políticas y los objetivos de seguridad y la experiencia práctica, y se reporta los resultados a la Dirección, para su revisión.

3.1. Métodos de Medición

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicarse a múltiples aspectos. Por su naturaleza, los métodos de medición pueden ser subjetivos u objetivos. Los métodos subjetivos implican el criterio humano, mientras que los objetivos se basan en una regla numérica, que puede ser aplicada por personas o recursos automatizados. Algunos ejemplos de métodos de medición son:

1. Encuestas/indagaciones.
2. Observación.
3. Entrevistas
4. Cuestionarios.
5. Evaluación de conocimientos.
6. Inspecciones.
7. Consulta a sistemas.
8. Supervisión
9. Muestreo.

Para la implementación de estos métodos en cualquier entidad hay disponibles diferentes procedimientos y herramientas que facilitan esta tarea, entre ellas:

1. Utilización de listas de verificación de la conformidad del SGSI con aspectos normados que requieren cumplirse.
2. La aplicación de programas diseñados con este objetivo, como por ejemplo el sistema de evaluación Diógenes elaborado por la Oficina de Seguridad para las Redes Informáticas.
3. La realización de diagnósticos de seguridad presenciales y remotos por especialistas de la propia organización o contratados a terceros.
4. La evaluación de los resultados obtenidos del análisis de los registros de auditoría generados por sistemas y servicios.

5. El análisis de los resultados de la supervisión del empleo de los sistemas y servicios por parte de los usuarios autorizados para ello.
6. Los reportes y alarmas generados por los sistemas de seguridad, como por ejemplo un Sistema de Detección de Intrusos (IDS por sus siglas en inglés).
7. El análisis de los incidentes de seguridad ocurridos a partir de la información registrada sobre estos.
8. El análisis de los reportes de las violaciones de los controles de seguridad.
9. El análisis de las no conformidades detectadas en controles realizados y su erradicación.

La medición sirve para cuestionar continuamente en base a datos y registros, si los controles de seguridad funcionan bien. Se establece un conjunto de indicadores que sirven para evidenciar que lo implementado funciona correctamente.

3.2. Indicadores de medición

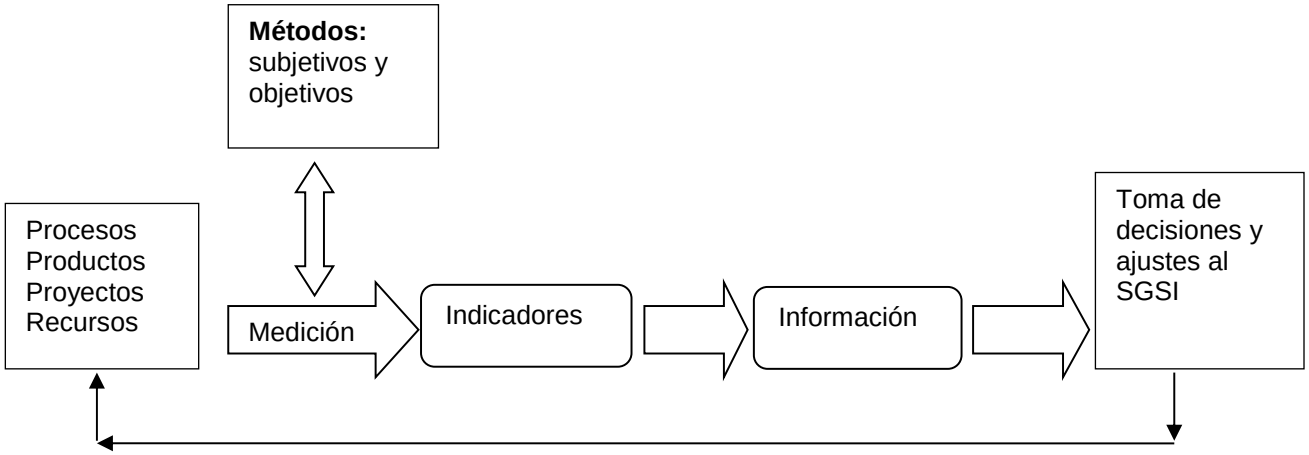
En esta etapa adquieren especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI.

Cada indicador tiene asociado valores que representen las metas a cumplir. En este sentido, cada organización define su criterio respecto a qué aspectos quiere controlar y medir para lograr el cumplimiento de los objetivos. Para ello se pueden definir distintos grupos de indicadores que recojan los diferentes ámbitos que se quieren gestionar. Por tanto, se podrían tener:

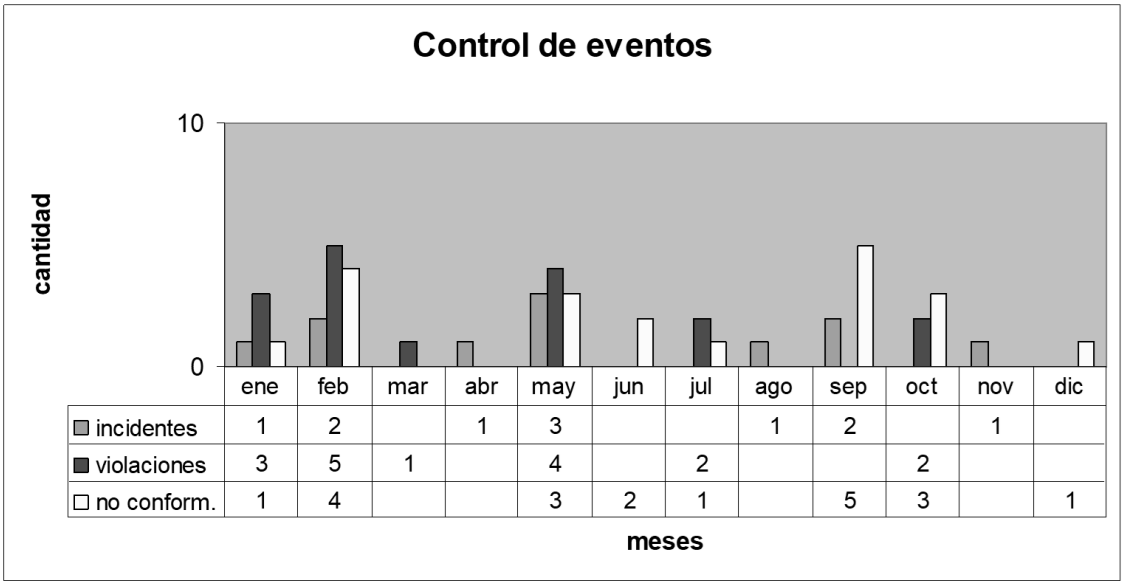
1. **Indicadores del grado de efectividad de los controles de seguridad:** Su sentido es valorar si los controles implantados funcionan bien o es necesario ajustarlos.
2. **Indicadores de medición del entorno y la hostilidad:** Su misión es detectar cambios en el entorno y contexto que rodea al SGSI para realizar ajustes respecto al análisis de riesgos por aparición de nuevas amenazas o cambios en sus frecuencias de ocurrencia. Por ejemplo, la aparición de nuevas amenazas internas, cambios en el clima laboral de la organización, frecuencia de publicación de vulnerabilidades, detección de nuevas aplicaciones malware.
3. **Indicadores de gestión interna:** Estos se establecen para evaluar el funcionamiento propio del propio SGSI y tiene que ver con la monitorización de las tareas propias de gestión. Por ejemplo, las relacionadas con la eliminación en plazo de no conformidades, el porcentaje de cumplimiento de los objetivos planteados, el número de no conformidades detectadas por auditoría.

Al definir y valorar el comportamiento de los indicadores, se tiene muy en cuenta el daño derivado de la ocurrencia de un incidente y su posible impacto en los objetivos de la organización.

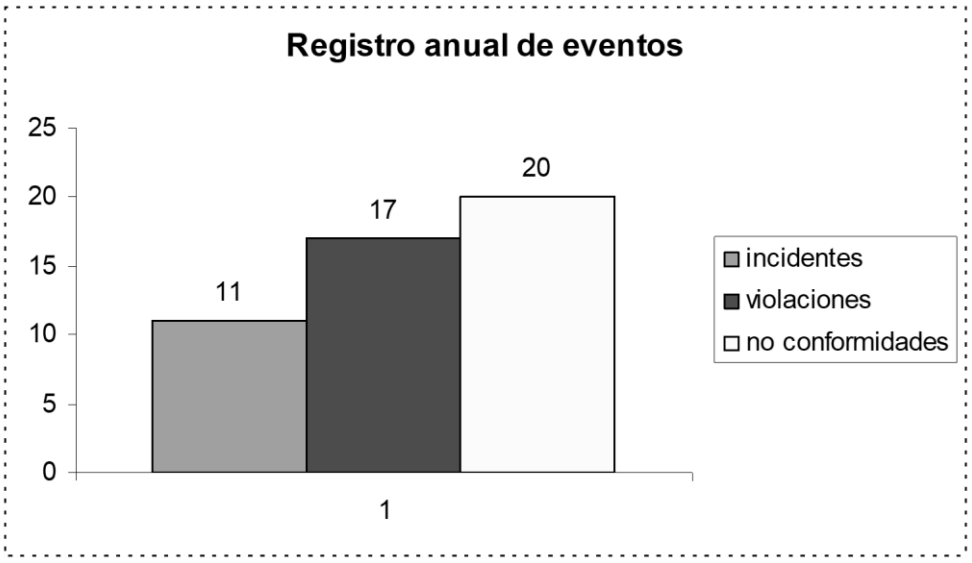
La información referente a estos indicadores, desde la perspectiva de la gestión, es la más crítica, dado que es la base de la retroalimentación del sistema. Por tanto, hay que disponer de sensores de diferente naturaleza y con diferentes objetivos: medir la evolución de la ejecución del plan, valorar el rendimiento y funcionamiento de las medidas de seguridad, vigilar el entorno por si se vuelve más hostil y otros.



Al final lo importante es no perder el sentido del por qué se hacen las cosas. Para ello, toda esta información se transforma en unas sencillas gráficas que la Dirección pueda entender y que sirvan como el auténtico "termómetro de la situación". Estos datos, adecuadamente procesados y visualmente representados, sin disponer de excesivos detalles y conocimientos técnicos, permiten a la Dirección realizar su principal labor dentro del SGSI: tomar decisiones y realizar los ajustes necesarios para el logro de los objetivos. A modo de ejemplo se muestra a continuación una tabla y un gráfico con datos de tres indicadores seleccionados:



	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
incidentes	1	2		1	3			1	2		1	
violaciones	3	5	1		4		2			2		
no conform.	1	4			3	2	1		5	3		1



Otro aspecto a tener en cuenta es el de la frecuencia. Se definen y programan claramente los intervalos en los cuales se lleva a cabo cada medición (semanal, mensual, trimestral, anual y otros.), se considera una relación entre la necesidad de contar con esta información y el esfuerzo para obtenerla (costo/beneficio).

Se puede definir un total de factores a evaluar (que nombraremos como K) y ver cuántos de ellos se cumplen (que nombraremos como k).

Por ejemplo: De 10 factores predeterminados se cumplen 7

K = 10 y k = 7
7/10 = 0.7 => 70 %

Algunas posibles relaciones para indicadores pudieran ser:

a) tiempo sin interrupciones/Tiempo total de servicio;
b) tiempo sin violaciones reportadas/Tiempo total de servicio;
c) 1/cantidad de incidentes computacionales;
d) velocidad real/velocidad contratada;
e) no conformidades detectadas/total de aspectos verificados.

3.3. Reglas que cumple una buena métrica:

1. Ser objetivas: aportan un criterio de recogida de datos medible y objetivo, que no dependa de valoraciones subjetivas.
2. Ser fáciles de obtener: Los datos sencillos, simples de calcular y poco costosos de recoger son buenos candidatos a ser métricas. Al respecto, lo más sencillo es recurrir a datos proporcionados por herramientas o procesados de forma automatizada.

3. Expresables de forma numérica o porcentual. No se basan en etiquetas cualitativas tales como "alto", "medio" o "bajo".
4. Expresable con el uso de algún tipo de unidad de medida: Siempre están vinculadas a algo tangible basado en escalas como el tiempo, número de defectos, o cuantías económicas.
5. Significativas: Toda buena métrica es significativa, es relevante para el hecho o circunstancia que se desea medir y aporta criterio. Una métrica que no aporta información no es una buena métrica y es desechada.

4. Proceso de Actualización del SGSI

Mantenimiento, mejora y corrección del SGSI

Objetivo principal: Realizar los cambios que sean necesarios para mantener el máximo rendimiento del SGSI

El proceso de actualización del SGSI comprende la aplicación de acciones correctivas y preventivas, basadas en los resultados del proceso de verificación descrito en el apartado anterior, para lograr la mejora continua.

En esta etapa se llevan a cabo las labores de mantenimiento del sistema, así como las acciones de mejora y de corrección identificadas si, tras la verificación, se ha detectado algún punto débil. Este proceso se suele llevar en paralelo con la verificación y se actúa al detectarse la deficiencia, no se espera a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

El SGSI se mantiene eficiente durante todo el tiempo y se adapta a los cambios internos de la organización, así como los externos del entorno. Para lograr el perfeccionamiento constante del SGSI se aplican las lecciones aprendidas de las experiencias de seguridad de otras organizaciones, las de la propia entidad y la de los incidentes ocurridos.

Durante la Implementación de los resultados derivados de la verificación se requiere, generalmente, modificar controles e implantar las mejoras identificadas en las revisiones del SGSI a partir de las decisiones sobre los cambios requeridos para mejorar el proceso y en consecuencia se:

1. Estandarizan los cambios de procesos.
2. Comunican los cambios a todos los implicados.
3. Proporciona entrenamiento al personal sobre los nuevos métodos.
4. Evalúan los nuevos riesgos.
5. Modifica el SGSI.
6. Actualiza el PSI.

Se comunican las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias, se precisa sobre cómo proceder ante el nuevo escenario y se entrena al personal con el fin de asegurar que las mejoras logren los objetivos previstos.

Algunos ejemplos de circunstancias que implican la necesidad de un nuevo análisis de riesgos pudieran ser las siguientes:

1. Instalación de nuevos tipos de redes (por ejemplo una red inalámbrica) en áreas de la entidad o de algún nuevo enlace para la comunicación con otras instancias.
2. Cambios en la topología de las redes o en la arquitectura de seguridad.
3. Introducción de tecnologías que no se habían empleado con anterioridad.
4. Incremento del empleo de soportes removibles como portadores de información por parte del personal.
5. Ocurrencia de algún incidente de seguridad.
6. Puesta en marcha de una nueva aplicación o introducción de un nuevo servicio de red.
7. Nuevos requerimientos informativos para la organización.
8. Incorporación de personal con poca experiencia y conocimientos.
9. Cambios en la plantilla de personal, en su composición o completamiento.
10. Conversión de locales de uso interno en áreas de acceso público.
11. Modificaciones estructurales de los inmuebles o cambios en su distribución.

Una vez realizados los cambios necesarios para mantener el máximo rendimiento del SGSI, se actualiza el PSI en las partes que corresponda e informan de ello a todos los que requieran conocerlo.

Segunda Parte: Estructura y contenido del Plan de Seguridad Informática

Consideraciones Generales

Para la elaboración del Plan de Seguridad Informática se tienen en cuenta las consideraciones siguientes:

1. El PSI es un documento de trabajo y como tal es accesible a todo el personal que requiera su utilización, por lo que la información que en él se incluye es ordinaria. No se incluye en este, información limitada o clasificada, la cual, de ser necesario, forma parte de un documento independiente que es categorizado conforme con lo establecido en la legislación vigente en materia de seguridad y protección de la información oficial.
2. El PSI se ajusta en todo momento al sistema de seguridad diseñado e implementado, se evitan formalismos y definiciones conceptuales y se utilizan como una herramienta de trabajo para la gestión de la seguridad.
3. Su redacción es simple, clara y libre de ambigüedades para que sea comprensible por todos los involucrados en su cumplimiento.
4. Tiene un carácter impositivo por lo que se evitan términos tales como “se recomienda”, “se debe” y otros similares que no implican obligatoriedad.
5. Contiene las tablas, gráficos y otros complementos que contribuyan a su mejor interpretación.
6. Se mantiene permanentemente actualizado sobre la base de los cambios que se produzcan en las condiciones consideradas durante su elaboración.

Presentación del Plan de Seguridad Informática

La página inicial (portada) contiene el título siguiente: "**PLAN DE SEGURIDAD INFORMATICA**" seguido de la denominación de la entidad. En la segunda página se consignan los datos referidos a la elaboración, revisión y aprobación del Plan de Seguridad Informática, de acuerdo con el formato siguiente:

	Elaborado	**Revisado**	**Aprobado**
Nombre			
Cargo			
Firma			
Fecha			

En la columna "**elaborado**" se consignan los datos de la persona que dirigió el equipo que confeccionó el Plan de Seguridad Informática, en la columna "**revisado**" los de la persona designada para su revisión antes de presentarlo a aprobación y en la columna "**aprobado**" se reflejan los datos del jefe de la entidad en la que el Plan tiene vigencia.

Estructura del Plan de Seguridad Informática

Los componentes del PSI se estructuran de la forma siguiente:

1. Alcance del PSI.
2. Caracterización del Sistema Informático.
3. Resultados del análisis de riesgos.
4. Políticas de Seguridad Informática.
5. Responsabilidades.
6. Medidas y Procedimientos de Seguridad Informática
   6.1. Clasificación y control de los bienes informáticos.
   6.2. Del Personal.
   6.3. Seguridad Física y Ambiental.
   6.4. Seguridad de Operaciones.
   6.5. Identificación, Autenticación y Control de Acceso.
   6.6. Seguridad ante Programas Malignos.
   6.7. Respaldo de la Información.
   6.8. Seguridad en Redes.
   6.9. Gestión de Incidentes de Seguridad.
7. Anexos del Plan de Seguridad informática.
   7.1. Listado nominal de usuarios.
   7.2. Registros.
   7.3. Control de cambios.

1. Alcance del Plan de Seguridad Informática

El primer asunto que se define en el PSI es su espacio de aplicación, o sea su alcance. El alcance expresa el radio de acción que abarca el Plan, de acuerdo con el Sistema Informático objeto de protección, para el cual fueron determinados los riesgos y diseñado el Sistema de Seguridad. La importancia de dejar definido claramente el alcance del Plan (y de ahí su inclusión al comienzo de este) consiste en que permite tener, a priori, una idea precisa de la extensión y los límites en que este tiene vigencia.

A modo de ejemplo, la definición del alcance del PSI en una entidad hipotética (Empresa X) podría ser:

"El presente Plan de Seguridad Informática es aplicable en su totalidad en las áreas de la Oficina Central de la Empresa X que se encuentran en el edificio situado en la calle Martí No. 610, entre Céspedes y Agramonte, La Habana.

Las políticas expresadas en este plan son de obligatorio cumplimiento para todo el personal de la Empresa X, incluyen los de sus dependencias que se encuentran en los municipios Plaza, Playa y Cerro".

2. Caracterización del Sistema Informático

Se describe de manera detallada el sistema informático de la entidad, precisan los elementos que permitan identificar sus particularidades y las de sus principales componentes: la información, las tecnologías de información, las personas y los inmuebles, y se considera entre otros:

1. Bienes informáticos, su destino e importancia.
2. Redes instaladas, estructura, tipo y plataformas que utilizan.
3. Aplicaciones en explotación.
4. Servicios informáticos y de comunicaciones disponibles.
5. Características del procesamiento, transmisión y conservación de la información, se tiene en cuenta el flujo interno y externo y sus niveles de clasificación.
6. Características del personal vinculado con las tecnologías y sus servicios, en particular su preparación, profesionalidad y experiencia.
7. Condiciones de las edificaciones, su ubicación, estructura, disposición de los locales y condiciones constructivas.

Al describir el sistema informático se emplean los esquemas, tablas, gráficos y otros medios auxiliares que se requieran; a fin de facilitar una mejor comprensión. Estos medios auxiliares pueden ser insertados, dentro de esta propia sección o al final del plan, como anexos a los cuales se hace obligada referencia.

La caracterización del sistema informático permite conocerlo con plenitud, facilita una mejor determinación de las necesidades de protección y evita pérdida de tiempo e imprecisiones. Su

descripción en detalle posibilita al que la lea tener un conocimiento lo más exacto posible de este, aunque sea la primera vez que se enfrente a él, cuestión que es de gran utilidad cuando se producen cambios en el personal, lo que suele ocurrir con relativa frecuencia.

Un ejemplo de caracterización del sistema informático de la Empresa X podría ser:

"El sistema informático de la Empresa X está soportado en los medios informáticos que se describen en el Anexo No. 1, que incluyen servidores, computadoras de mesa y portátiles, gran parte de ellas conectadas en red.

En la Oficina Central existe una red local que abarca las áreas situadas en la planta baja y los pisos 4 y 5 del edificio de la calle Martí No. 610.

Para la gestión de la red se cuenta con 5 servidores que utilizan como sistema operativo Windows 2003 Enterprise y Linux Debian; en las estaciones de trabajo se emplea Windows XP y Linux Ubuntu.

Los servidores tienen la función de: controlador de dominio, aplicaciones, base de datos, correo electrónico y Proxy.

Los servicios implementados en la red son navegación Internet, correo electrónico y transferencia de ficheros. La navegación y el correo tienen alcance nacional o internacional en dependencia de lo aprobado para cada usuario a partir de sus necesidades.

Las aplicaciones y bases de datos en explotación son:

- *Sistema de Representación Geoespacial (SIRGE)*
- *Sistema Contable (CONTAB)*
- *Sistema de Control de Información Clasificada (SCIC)*
- *Sistema de Control de Componentes (Everest).*
- *Sistema de Control de Actualizaciones (WSUS)*

Además se utilizan los paquetes de Office y Open Office para la elaboración de informes y otros documentos, en las máquinas previstas para el trabajo interno.

El cableado de la red está soportado por cable UTP categoría 5, 100 Mbits, con topología estrella (Anexo 2), protegido con canaletas. Las estaciones de trabajo se agrupan por áreas y pisos a partir de conmutadores (switchs) capa 2.

Además se cuenta con un punto de acceso inalámbrico (Access Point) a la red de Internet en el salón de reuniones del quinto piso.

La conexión con el exterior se realiza con el uso de una línea arrendada de 1 Mbit conectada directamente al proveedor de servicios de Internet.

El intercambio de información tanto interna como externa se realiza básicamente a través del correo electrónico.

La información ordinaria de la Oficina Central se procesa en las estaciones de trabajo de la red y la información clasificada en máquinas independientes, ubicadas en la Dirección de la Empresa, en el Departamento de Cuadros y en el de Seguridad y Defensa. La información recibida desde las dependencias de la empresa y la que se envía al Organismo superior se tramita por medio del correo electrónico y de la Intranet. La información que se expone en la Intranet es en todos los casos de uso público.

El edificio de Martí 610 se encuentra cerca del litoral habanero, tiene buenas condiciones constructivas, adecuadas tanto para la protección como para la preservación de los equipos y la posibilidad de visibilidad de las pantallas desde el exterior es prácticamente nula.
El personal que opera los equipos posee los conocimientos y la preparación necesaria para su empleo y en la mayor parte de los casos tiene nivel medio o superior."

3. Resultados del análisis de riesgos

Una vez definido el alcance del PSI y realizada una detallada descripción del sistema informático, corresponde finalizar esta primera parte con la formulación de las conclusiones obtenidas durante la determinación de las necesidades de protección, mediante la evaluación de los riesgos. Estas conclusiones incluyen:

a) Cuáles son los bienes informáticos más importantes para la gestión de la entidad y por lo tanto requieren de una atención especial desde el punto de vista de la protección; se especifican aquellos considerados de importancia crítica por el peso que tienen dentro del sistema;
b) qué amenazas pudieran tener un mayor impacto sobre la entidad en caso de materializarse sobre los bienes a proteger;
c) cuáles son las áreas con un mayor peso de riesgo y qué amenazas lo motivan.

Un ejemplo de los resultados del análisis de riesgos en la Empresa X podría ser:

Los bienes informáticos más importantes a proteger son:

- *La red de trabajo interno de la Oficina;*
- *El servidor de aplicaciones;*
- *Las bases de datos del sistema SIRGE (de importancia crítica);*
- *Las bases de datos de la intranet;*
- *El servicio de correo electrónico;*
- *El sistema contable CONTAB.*

Las amenazas más importantes a considerar de acuerdo con el impacto que pudieran tener sobre la empresa son:

- *El acceso no autorizado a la red, tanto producto de un ataque externo como interno.*

- *Pérdida de disponibilidad.*
- *La sustracción, alteración o pérdida de datos.*
- *Fuga de información clasificada.*
- *La introducción de programas malignos.*
- *El empleo inadecuado de las tecnologías y sus servicios.*
- *Las penetraciones del mar.*

Las áreas sometidas a un mayor peso/riesgo y las amenazas que lo motivan son:

- *El local de los servidores de la red (acceso no autorizado y pérdida de disponibilidad).*
- *El local de Economía (alteración o pérdida de datos, pérdida de disponibilidad y la introducción de programas malignos).*
- *El Departamento de Investigación y Desarrollo (alteración o pérdida de datos, pérdida de disponibilidad y la introducción de programas malignos).*
- *Las oficinas de la Dirección, del Departamento de Cuadros y del Departamento de Seguridad y Defensa (fuga de información clasificada).*
- *El almacén situado en la planta baja del edificio (penetraciones del mar).*

En la medida en que las conclusiones del análisis de riesgos sean más precisas se logra una visión más acertada de hacia dónde son dirigidos los mayores esfuerzos de seguridad y por supuesto los recursos disponibles para ello, y se logra que esta sea más rentable.

4. **Políticas de Seguridad Informática**

En esta sección se definen los aspectos que conforman la estrategia a seguir por la Entidad sobre la base de sus características, de conformidad con la política vigente en el país en esta materia y el sistema de seguridad diseñado.

Establecen las normas generales que cumple el personal que participa en el sistema informático y se derivan de los resultados obtenidos en el análisis de riesgos y de las definidas por las instancias superiores en las leyes, resoluciones, reglamentos, y otros documentos rectores.

Al definir las políticas de Seguridad Informática que son establecidas en la entidad se consideran los elementos expuestos en el punto No. 1.4.1 de la Primera Parte de esta Metodología.

Las políticas que se describan comprenden toda la organización, ya que es obligatorio su cumplimiento en las áreas que las requieran, razón por las que son lo suficientemente generales y flexibles para poder implementarse, en cada caso, mediante las medidas y procedimientos que demanden las características específicas de cada lugar.

A modo de ejemplo se muestran algunas de las políticas definidas en la Empresa X:

1. *Las propuestas de iniciativas encaminadas a mejorar el sistema de seguridad informática se aprueban por el Consejo de Dirección.*

2. *El acceso a las tecnologías de la entidad es expresamente aprobado en cada caso y el personal tiene que estar previamente preparado en los aspectos relativos a la seguridad informática.*

3. *Los usuarios de las tecnologías de la información y la comunicación responden por su protección y están en la obligación de informar cualquier incidente o violación que se produzca a su Jefe inmediato superior.*

4. *Todos los bienes informáticos son identificados y controlados físicamente hasta nivel de componentes.*

5. *Se establecen procedimientos que especifiquen quién y cómo se asignan y suspenden los derechos y privilegios de acceso a los sistemas de información.*

6. *Se prohíbe vincular cuentas de correo electrónico de la entidad a un servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través de este.*

7. *En caso de violación de la seguridad informática, se comunica al Jefe inmediato superior y a la Oficina de Seguridad para las Redes Informáticas y se crea una comisión encargada de analizar lo ocurrido y proponer la medida correspondiente.*

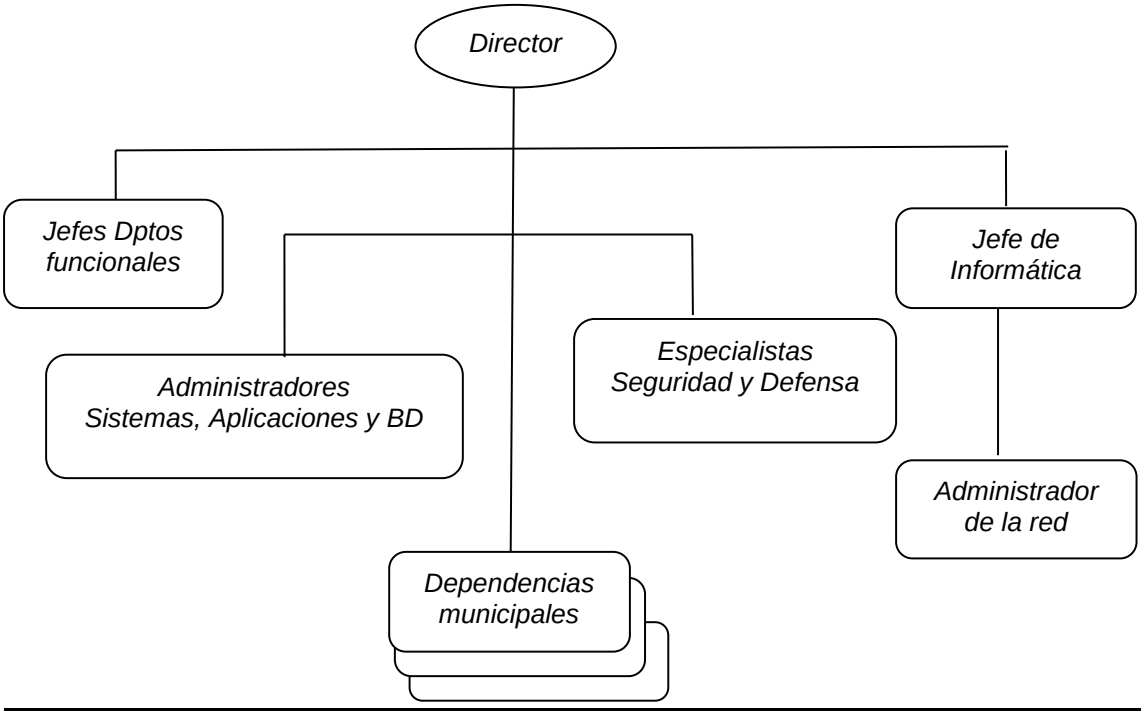
5. Responsabilidades

Se describe la estructura concebida en la Entidad para la gestión de la Seguridad Informática, se especifican las atribuciones, funciones y obligaciones de las distintas categorías de personal, que incluyen: directivos a los distintos niveles (jefe de la entidad, jefes de departamentos, áreas y grupos de trabajo o estructuras equivalentes); jefes y especialistas de informática; administradores de redes, sistemas y aplicaciones; especialistas de seguridad informática y de seguridad y protección y usuarios comunes de las tecnologías de Información.

Al especificar las atribuciones, funciones y obligaciones del personal en función de sus cargos, se tiene en cuenta lo establecido al respecto en el Reglamento de Seguridad para las TIC.

Un ejemplo de la estructura concebida para la gestión de la seguridad informática y de las funciones y obligaciones de los administradores de sistemas, aplicaciones y bases de datos en la Empresa X podría ser:

Estructura de gestión de la seguridad informática de la Empresa



Funciones y Obligaciones de los Administradores de Sistemas, Aplicaciones y Bases de Datos de la Empresa X.

a) *Informar a los usuarios de los controles de seguridad que hayan sido establecidos y verificar su utilización apropiada;*
b) *controlar el acceso a los sistemas, aplicaciones y bases de datos en correspondencia con la política establecida;*
c) *garantizar la ejecución de los procedimientos de salva de programas y datos, así como su conservación;*
d) *detectar posibles vulnerabilidades en los sistemas y aplicaciones bajo su responsabilidad y proponer acciones para su solución;*
e) *garantizar su mantenimiento y actualización y el registro de los sistemas y aplicaciones que lo requieran.*

Aplicaciones, Sistemas y Bases de Datos	***Administrador (poner nombres)***
Sistema de Representación Geoespacial (SIRGE)	*Jesús*
Sistema de Control de Componentes (Everest)	*Julio*
Sistema contable CONTAB	*Anaibis*
Sistema de control información clasificada (SCIC)	*Diana*
Sistema de Control de Actualizaciones (WSUS)	*Humberto*

6. Medidas y Procedimientos de Seguridad Informática

En este segmento del PSI se describe **cómo** se implementan, en las áreas a proteger, las políticas que han sido definidas para la entidad, en correspondencia con las necesidades de protección en cada una de ellas, de acuerdo con sus formas de ejecución, periodicidad, personal participante y medios**.** Se describen por separado los controles de seguridad implementados, en correspondencia con su naturaleza, se combinan el empleo de los recursos humanos y de los medios técnicos con las acciones que son realizadas.

Las medidas y procedimientos no deben confundirse con una declaración de intención o línea de deseos, por lo que con su descripción se especifican los controles implementados, no los que se quisieran implementar.

El PSI se sustenta sobre la base de los recursos disponibles y en dependencia de los niveles de seguridad alcanzados y de los aspectos que queden por cubrir se elabora un Programa de Desarrollo de la Seguridad Informática, que incluya las acciones a realizar por etapas para lograr niveles superiores (ver punto No. 2.1. de la Primera Parte).

Hay que concentrarse en las acciones que garantizan la instrumentación de las políticas definidas y su aplicación apropiada en cada área que lo requiere.

6.1. Clasificación y control de los bienes informáticos

Estas medidas y procedimientos persiguen identificar los bienes informáticos de acuerdo con su importancia, controlar y supervisar que sean utilizados en funciones propias del trabajo y garantizar su protección. En este apartado se incluyen las medidas y los procedimientos que se requieran para:

1. Precisar los métodos de supervisión y control que se utilicen, el personal encargado de ejecutarlos y los medios empleados para ello.
2. Establecer los mecanismos que se requieran para identificar y controlar los bienes informáticos y la conformación de su inventario permanentemente actualizado.
3. Precisar la persona encargada de cada bien informático y responsable por su protección.
4. Garantizar la autorización y el control sobre el movimiento de los bienes informáticos.

A modo de ejemplo de medidas y procedimientos de control de los medios informáticos se muestran los siguientes:

Medida:
La administradora del sistema CONTAB responde por la integridad de los medios destinados para la explotación de esta aplicación.

Procedimiento 1 *Control de medios informáticos.*

1. *Acceder la última semana de cada mes al Sistema de Control de Componentes (Everest) a través del servidor de la red y se aplica a los medios informáticos que forman parte del dominio de la red.*

2. *Comprobar cambios existentes desde el último control realizado.*
3. *Informar a la Dirección de la Empresa los resultados de la comprobación.*
4. *Generar un resumen de los resultados de cada control y conservarlo por un año.*
   Responsable: *Administrador de la red*
5. *Esclarecer en caso de existir diferencia, las causas y responsabilidades.*
   Responsable: *Director de la empresa*

6.2. Del Personal

Las medidas y procedimientos asociadas con el personal tienen como objetivo garantizar el cumplimiento de las funciones y responsabilidades de seguridad generales y específicas de las personas vinculadas con las TIC y sus servicios, así como la documentación de estas y aseguran:

1. La selección adecuada del personal previsto para ocupar cargos en la actividad informática o con acceso a sistemas críticos, a información de valor o a la supervisión y seguridad de los sistemas.
2. La obligación de la entidad en cuanto a la preparación del personal y la responsabilidad del trabajador hacia la Seguridad Informática, así como la inclusión de estos aspectos en los términos y condiciones del contrato de empleo.
3. La forma en que es autorizada por la dirección de la entidad la utilización de las tecnologías y sus servicios por parte de los usuarios que lo necesiten.
4. La obligación de los jefes a cada nivel en cuanto a garantizar la Seguridad Informática en su área de responsabilidad.
5. Las acciones a realizar en caso de empleo no autorizado de las tecnologías y sus servicios por parte de los usuarios.
6. La responsabilidad de los jefes a cada nivel en cuanto a la preparación de su personal y del conocimiento de sus deberes y derechos, incluyen la introducción en el contrato de trabajo de la constancia del compromiso de cada trabajador.
7. Los requerimientos de seguridad para la autorización del acceso a las tecnologías y servicios por parte de personal externo.
8. Las formas y medios mediante los cuales los usuarios informan acerca de cualquier incidente de seguridad, debilidad o amenaza.
9. Evitar la realización de acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros, así como la introducción, ejecución, distribución o conservación de programas para esos fines o información contraria al interés social, la moral y las buenas costumbres.

Los controles de seguridad en relación con el personal consideran no solo los requisitos a cumplir por los trabajadores durante el tiempo de vigencia de su contrato de empleo, sino también antes de ser contratado y con posterioridad al cese de su relación laboral.

Un ejemplo de procedimiento relacionado con el personal en la Empresa X podría ser:

Procedimiento 2 *Aprobación de acceso a las tecnologías y servicios por parte de personal externo.*

1. *Elaborar y presentar la solicitud de autorización de acceso a las TIC al Director de la Empresa, donde se incluya el nombre y apellidos de la persona que necesita el acceso y su número de carné de identidad; las razones que justifican este acceso, el acceso que se requiere y el tiempo que se requiera mantenerlo.*
   Responsable: *Jefe del área asociada con el acceso*
2. *Aprobar (denegar) la solicitud en caso que corresponda, y darlo a conocer por escrito al administrador de la red, al Jefe del área que realizó la solicitud y al Jefe del Departamento de Seguridad y Defensa, especifican el alcance del acceso y su tiempo de vigencia.*
   Responsable: *Director de la Empresa*
3. *Asignar (en caso de autorización de acceso), un identificador personal y único para el acceso a los sistemas y servicios determinados en la aprobación y definir en el servidor de la red los atributos en correspondencia con la autorización otorgada.*
   Responsable: *Administrador de la red*
4. *Imponer a la persona a que se otorga el acceso de sus obligaciones y atribuciones en relación con el empleo de las tecnologías y sus servicios.*
   Responsable*: Jefe del área que solicita el acceso*
5. *Solicitar al director la cancelación del acceso concedido e informar las razones de la solicitud.*
   Responsable: *Jefe del área que solicita el acceso*
6. *Cancelar la cuenta y los permisos de acceso una vez concluido el plazo previsto.*
   Responsable: *Administrador de la red.*

6.3. Seguridad Física y Ambiental

Las medidas y procedimientos de seguridad física y ambiental tienen como objetivo evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones, las tecnologías y la información de la organización.

Se aplican a los locales donde se encuentran las TIC y directamente a estas mismas tecnologías y a los soportes de información e incluyen: medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.

La protección física se alcanza con la creación de una o más barreras físicas alrededor de las áreas de procesamiento de la información. El uso de múltiples barreras brinda protección adicional, de modo que la falta de una barrera no significa que la seguridad se vea comprometida inmediatamente.

La protección del equipamiento (incluyen aquel utilizado fuera de la entidad) es necesaria para reducir el riesgo de accesos no autorizados a la información y para protegerlo contra pérdidas o daños. Se pueden requerir controles especiales para proteger contra amenazas físicas, y para preservar los equipos, tales como la garantía del suministro eléctrico y la infraestructura adecuada del cableado.

La seguridad ambiental incluye la aplicación de medios contra daños que puedan ser ocasionados por incendios, inundaciones, terremotos, explosiones, perturbación del orden, y otras formas de desastre natural o artificial.

Las medidas y procedimientos de seguridad física y ambiental van dirigidas a:

1. La protección de las tecnologías contra la sustracción o alteración, e incluyen sus componentes y la información que contienen.
2. Impedir su empleo para cometer acciones malintencionadas o delictivas.
3. Disminuir el impacto producido por fuego, inundación, explosión, perturbación del orden y otras formas de desastre natural o artificial.
4. La protección contra fallas de alimentación u otras anomalías eléctricas.
5. La protección de los cables que transporten datos o apoyen los servicios contra la intercepción o el daño.
6. Garantizar que el equipamiento reciba un mantenimiento adecuado en correspondencia con las especificaciones del fabricante.
7. El control del movimiento de las tecnologías.
8. La preservación de la información del equipamiento que cause baja o se destine a otras funciones.

Corresponde a esta parte del PSI la determinación de los locales considerados como áreas o zonas controladas, en correspondencia con la caracterización del sistema informático realizado y los resultados del análisis de riesgos y que por lo tanto tienen requerimientos específicos de seguridad, en base a lo cual se declaran áreas **limitadas, restringidas o estratégicas** y se describen las medidas que se aplican en cada una de ellas, por ejemplo: restricciones para limitar el acceso a los locales, procedimientos para el empleo de cierres de seguridad y dispositivos técnicos de detección de intrusos y otros.

Al referir las medidas y procedimientos que se establecen para lograr una seguridad física y ambiental adecuada a las necesidades de las TIC, no es necesario describir las condiciones constructivas de los inmuebles, pues ya eso ha sido realizado durante la caracterización del sistema informático y expuesto en el punto 2 de la estructura del PSI.

Un ejemplo de la clasificación y medidas específicas en las áreas controladas en la Empresa X es la siguiente:

Área controlada	***Categoría***	***Medidas específicas***
Dirección, Cuadros, Seguridad y Defensa	*Limitada*	*Acceso físico limitado; cierres seguros en puertas y ventanas; alarma contra intrusos.*
Economía	*Limitada*	*Acceso físico limitado; control de soportes removibles; alarma contra intrusos; separación de funciones; protección de las copias de programas y datos.*

Servidores de la red	*Limitada*	*Acceso solo a administradores; cierre magnético en la puerta de acceso y alarma contra intrusos: redundancia de HW, SW, climatización y datos.*
Investigación y Desarrollo	*Limitada*	*Acceso físico limitado; cierres seguros en puertas y ventanas; alarma contra intrusos; redundancia de datos.*

Se describen en detalle las medidas específicas de la tercera columna de la tabla anterior: a quien se autoriza el acceso, tipo de alarma, en que consiste el cierre seguro, como se controlan los soportes removibles, que funciones están separadas en usuarios diferentes, como se logra la redundancia y la protección de la información de respaldo y otros.

Obsérvese que las áreas declaradas como controladas coinciden con las que se determinó en el análisis de riesgos que estaban sometidas a un mayor peso de riesgo (ver punto 3 de la estructura del PSI, Resultados del análisis de riesgos).

En el próximo ejemplo se muestra una medida con el procedimiento correspondiente para el control del movimiento de las tecnologías:

Medida:

La entrada, salida y traslado de las TIC en la Empresa X se realiza con autorización del Director en correspondencia con el Procedimiento 3, dejan constancia de ello en el Registro1, movimiento de TIC.

Procedimiento 3 Movimiento de las TIC

1. *Solicitar autorización por escrito al Director de la Empresa X para el movimiento de las tecnologías que lo requieran, fundamentan en qué consiste el movimiento, los motivos y si es temporal el tiempo requerido.*
   ***Responsable:** Jefe del área a que pertenece el medio a trasladar*
2. *Autorizar si es procedente el movimiento de las tecnologías y darlo a conocer por escrito al Jefe del área que realizó la solicitud, al Jefe del área de Contabilidad y al Jefe del Departamento de Seguridad y Defensa, especifican el tiempo de vigencia de la autorización.*
   ***Responsable:** Director de la Empresa X*
3. *Registrar en el sistema CONTAB el movimiento del medio básico autorizado a trasladar.*
   ***Responsable**: Jefe del área de Contabilidad.*
4. *Revisar antes de su salida (entrada) de la entidad las tecnologías autorizadas a trasladar, precisan la existencia y estado de sus partes y componentes, si contienen información y de qué tipo, así como lo relacionado con el control antivirus.*
   ***Responsable:** Jefe del área a que pertenece el medio a trasladar*
5. *Consignar el movimiento en el Registro 1, especifican la fecha en que se produce, los datos del equipo objeto del movimiento, de qué lugar se extrae o proviene y a qué lugar se lleva y motivo por el que se realiza el movimiento (evento, exposición, reparación y otros.).*
   ***Responsable:** Jefe del área a que pertenece el medio a trasladar*
6. *Controlar el cumplimiento de las autorizaciones sobre el movimiento de las tecnologías y su registro adecuado.*

Responsable: *Jefe del Departamento de Seguridad y Defensa*

6.4. Seguridad de Operaciones

Las medidas y procedimientos de Seguridad de Operaciones están dirigidas a lograr una eficiente gestión de la seguridad y garantizan el cumplimiento de las regulaciones vigentes en el país, así como las establecidas por la propia entidad.

La gestión del sistema de seguridad implica el control de las acciones que se realizan dentro del sistema informático y su garantía de que se ajustan a las políticas de seguridad establecidas para el empleo de las tecnologías y sus servicios, y para ello las medidas y procedimientos de seguridad de operaciones consideran, entre otros, los aspectos siguientes:

1. La aplicación del principio de separación de funciones evita que se asignen a una misma persona tareas que en su conjunto pueden propiciar la modificación no autorizada de datos o el mal uso de los sistemas.
2. La aprobación para la introducción en la entidad de nuevos sistemas informáticos, actualizaciones y nuevas versiones, previa verificación de su correspondencia con el sistema de seguridad establecido y el cumplimiento de los criterios de seguridad apropiados.
3. El control por el personal autorizado de las acciones necesarias para cubrir las brechas de seguridad y la corrección de los errores de los sistemas, su documentación y reporte a quienes corresponda.

En esta parte del PSI se incluye la ejecución de los procedimientos de revisión mediante los métodos de medición que posibiliten detectar errores de proceso, identificar fallos de seguridad de forma rápida y determinar las acciones a realizar para lograr el ciclo de mejora continua. Se utilizan para ello los indicadores seleccionados sobre la base de los criterios respecto a qué aspectos se controlan y miden para lograr el cumplimiento de los objetivos planteados en el SGSI implementado en la entidad. Existen diversos métodos de medición y hay disponibles diferentes procedimientos y herramientas que facilitan su implementación en cualquier entidad (ver punto 3 de la Primera Parte, Proceso de Verificación del SGSI).

Se incluyen además las medidas y procedimientos implementados para el registro y análisis de las trazas de auditoría generadas por los sistemas operativos y servicios de redes, y por los sistemas instalados según lo reglamentado, con el fin de monitorear las acciones que se realicen (acceso a ficheros, dispositivos, empleo de los servicios y otros), y detectar indicios de hechos relevantes a los efectos de la seguridad que puedan afectar la estabilidad o el funcionamiento del sistema informático.

En caso de empleo de software especializado que permita la detección de posibles errores de configuración u otras vulnerabilidades, así como su corrección, se describen los procedimientos requeridos.

Se refieren además las medidas que garanticen la integridad de los mecanismos y registros de auditoría limitan su acceso solo a las personas autorizadas para ello.

A modo de ejemplo de procedimiento de las acciones necesarias para cubrir las brechas de seguridad y la corrección de los errores en la Empresa X se muestra el siguiente:

***Procedimiento 4* Corrección de errores y brechas de seguridad.**

1. *Instalar y configurar las aplicaciones Wsus, destinada para distribuir parches de seguridad de Microsoft para la eliminación de vulnerabilidades conocidas cuando su solución sea publicada por el fabricante y LANguard y Nmap, para detectar brechas de seguridad, puertos abiertos y otras vulnerabilidades similares.*
   ***Responsable:** Administrador de la red*
2. *Ejecutar las aplicaciones LANguard y Nmap una vez al mes y controlar cada lunes la ejecución de Wsus.*
   ***Responsable:** Administrador de la red*
3. *Informar los resultados de las acciones de corrección de errores y brechas de seguridad al Jefe del Departamento de Informática cada vez que se realicen y preservar los registros en los soportes habilitados al efecto por un tiempo no menor de un año.*
   ***Responsable:** Administrador de la red*
4. *Analizar los resultados de las acciones de corrección de errores y brechas de seguridad y su correspondencia con lo previsto en el Sistema de Seguridad Informática de la Empresa y, en caso de detectarse nuevas vulnerabilidades, proponer las acciones necesarias para su evaluación y determinación de las modificaciones requeridas para su eliminación.*
   ***Responsable:** Jefe del Departamento de Informática*
5. *Actualizar los cambios en el PSI.*
   ***Responsable:** Jefe del Departamento de Informática*

6.5. Identificación, Autenticación y Control de Acceso

Las medidas y procedimientos de identificación, autenticación y control de acceso responden a las políticas que previamente fueron definidas en la entidad sobre estos aspectos, y tienen como objetivo gestionar el acceso a la información de forma segura, garantizan el acceso de usuarios autorizados e impiden el acceso no autorizado a los sistemas de información. Los accesos a la información y a las instalaciones de procesamiento de la información son controlados sobre la base de requisitos de seguridad. Los controles consideran:

a) Las políticas para la autorización y distribución de la información.
b) La consistencia entre los controles de acceso y las políticas de clasificación de la información.
c) La legislación vigente y las obligaciones contractuales con respecto a la protección del acceso a los datos o servicios.
d) El establecimiento de perfiles estándar de acceso de usuarios para roles comunes.
e) La gestión de derechos de acceso en un ambiente distribuido y de redes, que reconozca todos los tipos de conexión posibles.
f) La separación de roles de control de acceso, por ejemplo, solicitud de acceso, autorización de acceso y administración de acceso.
g) Los requisitos para autorizaciones formales de solicitudes de acceso.
h) La cancelación de derechos de acceso.

Esos controles cubren todas las etapas del ciclo de vida del acceso del usuario, desde el registro inicial de nuevos usuarios hasta la cancelación final del registro de usuarios que no requieren más acceso a los sistemas de información y a los servicios.

Identificación de usuarios

Los procedimientos de identificación de usuarios garantizan:

a) la utilización de un identificador único (ID) para cada usuario para permitir que queden vinculados y sean responsables de sus acciones;
b) la verificación de que el usuario tenga autorización para el uso del servicio o el sistema de información;
c) la verificación de que el nivel de acceso otorgado se corresponda con la necesidad de uso y que es consistente con la política de seguridad, por ejemplo que no compromete la segregación de tareas;
d) que los usuarios firmen declaraciones indica que ellos comprenden y asumen las condiciones de acceso;
e) mantener un registro impreso de todas las personas a las que se les otorga acceso;
f) eliminar inmediatamente o bloquear los derechos de acceso de los usuarios que hayan cambiado roles o tareas o dejado la organización; y
g) realizar periódicamente una verificación para eliminar o bloquear las cuentas e identificadores de usuarios (ID´s) redundantes.

Se explica el método empleado para la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes, y se especifica:

1. Cómo se asignan los identificadores de usuarios.
2. Si existe una estructura estándar para la conformación de los identificadores de usuarios.
3. Quién asigna los identificadores de usuarios.
4. Cómo se eliminan los identificadores de usuarios una vez que concluya la necesidad de su uso y cómo se garantiza que estos no sean utilizados nuevamente.
5. El proceso de revisión de utilización y vigencia de los identificadores de usuarios asignados.

Autenticación de usuarios

Se explica el método de autenticación empleado para comprobar la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes.

Cuando se utilice algún dispositivo específico de autenticación, se describe su forma de empleo. En el caso de empleo de autenticación simple por medio de contraseñas se especifica:

1. Cómo son establecidas las contraseñas.
2. Tipos de contraseñas utilizadas (configuración de arranque, protector de pantalla, aplicaciones).

3. Estructura y periodicidad de cambio que se establezca para garantizar la fortaleza de las contraseñas utilizadas en los sistemas, servicios y aplicaciones, en correspondencia con el peso de riesgo estimado para estos.
4. Causas que motivan el cambio de contraseñas antes de que concluya el plazo establecido.

La estructura y periodicidad de cambio de las contraseñas de acceso son seleccionadas en correspondencia con la importancia de los bienes cuyo acceso se protege y los riesgos a que están sometidos, así como la existencia de otros tipos de controles complementarios que contribuyan a su protección, por lo que no necesariamente son iguales en todos los casos. Por ejemplo, para un sistema que no está catalogado como de importancia crítica para la entidad y que además está ubicado en un área a la que no acceden muchas personas, tal vez una contraseña de pocos caracteres que se modifique en intervalos largos sería suficiente, por el contrario un sistema de importancia crítica para la entidad cuenta con contraseñas de mayor fortaleza, se obliga a su cambio con mayor frecuencia.

En una red, con este objetivo podrían crearse grupos con necesidades de seguridad comunes, a los cuales se les impondrían requerimientos diferenciados en cuanto a la estructura y cambio de las contraseñas de acceso.

La instauración de contraseñas se controla a través de un proceso formal de gestión. El proceso incluye los requisitos siguientes:

a) exigir a los usuarios que firmen una declaración de que se comprometen a mantener confidencialidad sobre las contraseñas personales; esta declaración firmada se incluye dentro de los términos de empleo como parte de sus responsabilidades hacia la Seguridad Informática (ver punto 6.2 “Del Personal”);
b) establecer procedimientos para verificar la identidad del usuario antes de la utilización de cualquier contraseña;
c) cuando se asigne inicialmente una contraseña temporal, los usuarios son forzados a cambiarla inmediatamente después del primer acceso;
d) las contraseñas temporales son proporcionadas a los usuarios de un modo seguro y se evita el uso de mensajes de correo electrónico de terceras partes o no protegidos (en texto claro);
e) las contraseñas por defecto de los vendedores se cambian inmediatamente luego de la instalación del software o sistemas; y
f) las contraseñas son únicas para cada persona y no son descifrables.

Las contraseñas son un medio común de verificación de la identidad del usuario antes de acceder a los sistemas de información o a los servicios, de acuerdo con la autorización que tenga el usuario, pero es un método que puede ser violado con relativa facilidad. En los casos que se requiera una mayor seguridad, se consideran otras tecnologías disponibles para la identificación y autenticación del usuario, tales como biometría, por ejemplo, verificación de huella digital, verificación de firma, y uso de medios físicos de autenticación como tarjetas inteligentes.

Se exige a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas. Todos los usuarios son advertidos en cuanto a:

a) mantener confidencialidad sobre la contraseña;
b) evitar mantener un registro de contraseñas en texto claro en cualquier medio (por ejemplo, papel, archivo de software o dispositivo de mano);
c) cambiar las contraseñas cuando haya una indicación de riesgo en el sistema o en la contraseña;
d) seleccionar contraseñas de calidad con suficiente longitud mínima que sean:
   1. Fáciles de recordar.
   2. No se basen en algo que alguien pueda adivinar fácilmente o usen información relacionada con la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento, etc.
   3. No vulnerables a ataques tipo diccionario (es decir, que no consistan en palabras incluidas en diccionarios).
   4. Libres de caracteres idénticos sucesivos ya sean numéricos o alfabéticos.

e) Cambiar las contraseñas a intervalos regulares o basados en el número de accesos (las contraseñas de cuentas privilegiadas son cambiadas más frecuentemente que las contraseñas normales), y evitar la reutilización o reciclaje de contraseñas;
f) cambiar las contraseñas temporales en la primera conexión;
g) no incluir contraseñas en ningún proceso automatizado de conexión;
h) no compartir las contraseñas de usuario individuales; y
i) no utilizar la misma contraseña para propósitos de trabajo y particulares.

Control de acceso a los bienes informáticos

Se describen las medidas y procedimientos que aseguran el acceso autorizado a los bienes informáticos que requieren la imposición de restricciones a su empleo, se especifica:

1. A qué bienes informáticos se le implementan medidas de control de acceso.
2. Métodos de control de acceso utilizados.
3. Quién otorga los derechos y privilegios de acceso.
4. A quién se otorgan los derechos y privilegios de acceso.
5. Cómo se otorgan y suspenden los derechos y privilegios de acceso.

El control de acceso a los bienes informáticos está basado en una política de “mínimo privilegio”, en el sentido de otorgar a cada usuario solo los derechos y privilegios que requiera para el cumplimiento de las funciones que tenga asignadas.

La asignación de derechos y privilegios es controlada a través de procedimientos formales de autorización que determinan el perfil de cada usuario. Se consideran los elementos siguientes:

a) asociar el derecho de acceso con cada componente, por ejemplo sistema operativo, sistema de gestión de base de datos y de cada aplicación, identifican los usuarios a los que es necesario asignar tales privilegios;
b) los privilegios son asignados sobre la base de necesidad de uso y consideran recurso por recurso;

c) se implementa un proceso de autorización y se mantiene un registro de todos los privilegios asignados; los privilegios no se otorgan hasta que el procedimiento de autorización concluya.

Hay que tener en cuenta que el uso inapropiado de los privilegios de administración puede ser un factor importante de surgimiento de fallas o brechas de seguridad (cualquier característica o recurso de un sistema informático que habilite al usuario a hacer caso omiso de los controles de este o de la aplicación).

La dirección de la entidad instrumenta la revisión de los derechos de acceso de los usuarios a intervalos regulares para mantener un control efectivo sobre el acceso a los datos y servicios informáticos, utilizan un proceso formal que considere los siguientes aspectos:

a) los derechos de acceso de usuarios son revisados después de cualquier cambio, tal como el traslado de un cargo a otro dentro de esta organización, o el cese de las relaciones laborales; y
b) verificar que con la asignación de derechos no se obtienen privilegios no autorizados.

Como parte del control de acceso a los bienes informáticos se incluyen las medidas y procedimientos establecidos, con el fin de evitar la modificación no autorizada, destrucción y pérdida de los ficheros y datos, así como para impedir que sean accedidos públicamente, se especifican:

1. Medidas de seguridad implementadas a nivel de sistemas operativos, aplicación o ambos, para restringir y controlar el acceso a las bases de datos.
2. Medidas para garantizar la integridad del software y la configuración de los medios técnicos.
3. Empleo de medios criptográficos para la protección de ficheros y datos.

Ejemplo de procedimiento en la Empresa X

***Procedimiento 5* Aprobación y cancelación de acceso a las TIC**

1. *Elaborar y presentar la solicitud de autorización (cancelación) de acceso a las TIC al Director de la Empresa, donde se incluya el nombre y apellidos del trabajador que necesita el acceso; las razones que justifican este acceso y los activos a que solicita acceder. De ser una necesidad temporal especifica el tiempo que se requiera mantenerlo. En el caso de retiro del acceso presenta breve informe que refiere los motivos de la propuesta y si es definitiva o temporal.*
   ***Responsable:** Jefe del área a que pertenece el trabajador*
2. *Aprobar (denegar) la solicitud en caso que corresponda, y darlo a conocer por escrito al administrador de la red y al Jefe del área que realiza la solicitud, especifica el alcance del acceso.*
   ***Responsable:** Director de la Empresa*
3. *Preparar al trabajador en el uso adecuado de las TIC y en sus obligaciones como usuario de estas y firma por el trabajador del compromiso de empleo de estas. El documento original se entrega al administrador de la red y la copia se incluye en el contrato de trabajo.*
   ***Responsable:** Jefe del área a que pertenece el trabajador*
4. *Asignar (en caso de autorización de acceso), un identificador personal y único para el acceso a los sistemas y servicios determinados en la aprobación y definir en el servidor los atributos en correspondencia con la autorización otorgada.*
   ***Responsable:** Administrador de la red*

5. *Otorgar al usuario una contraseña temporal para ser utilizada en su primera conexión, se obliga a cambiarla una vez que acceda al sistema o servicio asignado.*
   Responsable: *Administrador de la red*
6. *Configurar en el servidor los atributos que se determinen o se agregan en correspondencia con la autorización otorgada.*
   Responsable: *Administrador de la red*
7. *Cancelar, en caso de revocación de acceso, la cuenta y los permisos de acceso otorgados.*
   Responsable: *Administrador de la red*
8. *Conservar las autorizaciones de acceso a las TIC en el área de informática por un período no menor de 1 año.*
   Responsable: *Jefe del Departamento de Informática*
9. *Realizar un control trimestral de este procedimiento e informar de sus resultados al Director de la Empresa.*
   Responsable: *Jefe del Departamento de Organización y Supervisión*

6.6. Seguridad ante programas malignos

Se establecen las medidas y procedimientos que se requieran para la protección contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para evitar su generalización, se especifican los programas antivirus utilizados y su régimen de instalación y actualización.

La protección contra códigos maliciosos se basa en el empleo de medidas de prevención, detección y recuperación, en la necesidad de la seguridad, y en controles apropiados de acceso al sistema. Las siguientes pautas son consideradas:

1. Establecimiento de políticas que instituyan la prohibición del uso de software no autorizado y la protección contra los riesgos asociados a la obtención de archivos y software por redes externas o cualquier otro medio, indican las medidas protectoras a adoptar.
2. Revisiones regulares del contenido de datos y software que soportan los procesos de gestión de la entidad y de la presencia de archivos no aprobados o modificaciones no autorizadas.
3. La instalación y actualización regular de programas antivirus que exploren las computadoras y los soportes de forma rutinaria o como un control preventivo para la detección y eliminación de código malicioso; las verificaciones incluyen:
   a) Comprobación de archivos en medios electrónicos u ópticos, y archivos recibidos a través de redes, para verificar la existencia de código malicioso, antes de su uso;
   b) comprobación de todo archivo adjunto a un correo electrónico o de cualquier descarga antes de su uso; realizar esta comprobación en distintos lugares, por ejemplo, en los servidores de correo, en las computadoras terminales o a la entrada de la red de la organización;
   c) comprobación de páginas Web para saber si existe en ellas código malicioso.

4. La definición de procedimientos y responsabilidades de gestión para la protección de los sistemas contra código malicioso, la capacitación para su uso, la información de los ataques de los virus y las acciones de recuperación.

5. La implementación de medidas para la recuperación ante ataques de código malicioso, incluyen los datos y software necesarios de respaldo y las disposiciones para la recuperación.
6. La implementación de procedimientos para obtener información sobre nuevos códigos maliciosos a través de listas de correo y comprobación de los sitios Web que brindan esa información.
7. La implementación de procedimientos para verificar la información relativa al software malicioso y asegurarse que es real; los encargados de esta actividad pueden diferenciar los códigos maliciosos reales de los falsos avisos de código malicioso, para lo que usan fuentes calificadas; se advierte al personal sobre el problema de los falsos avisos de código malicioso y qué hacer en caso de recibirlos.

Ejemplo de procedimiento en la Empresa X

***Procedimiento 6* Descontaminación de programas malignos**

1. *Al detectar en una estación de trabajo indicios de contaminación detener la actividad que se realiza, desconectarla de la red e informar al Jefe inmediato y al Administrador de la red.*
   Responsable: *Usuario de la estación de trabajo*
2. *Identificar de qué tipo de programa maligno se trata.*
3. *Verificar que en el medio contaminado se ejecuta una versión actualizada del programa antivirus instalado y de no cumplirse, proceder a la actualización del programa antivirus y llevar a cabo la descontaminación. De ser exitosa la descontaminación, poner en operación el medio afectado.*
4. *Revisar los soportes y el resto de las tecnologías que pudieran haber sido afectadas.*
5. *Investigar las causas de aparición del código malicioso.*
6. *Realizar las anotaciones pertinentes en el Registro de Incidencias (Registro No. 3).*
7. *Reportar el incidente a su instancia superior y a la OSRI.*
8. *Si es un programa maligno desconocido, proceder al aislamiento del fichero contaminado y remitirlo a la empresa Segurmática.*
   Responsable: *Administrador de la red*

6.7. Respaldo de la Información

Las medidas y procedimiento de respaldo que se implementen garantizan mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información frente a cualquier eventualidad.

Para alcanzar un nivel de respaldo adecuado se hacen las copias de seguridad de la información y del software que se determinen en cada caso y se comprueban regularmente.

Se dispone de procedimientos de respaldo para asegurar que toda la información esencial y el software puedan recuperarse tras un desastre o fallo, considerar para ello los elementos siguientes:

a) definir el nivel necesario de información de respaldo;
b) realizar copias seguras y completas de la información, y establecer los procedimientos de restauración;

c) determinar el grado (completo o parcial) y la frecuencia de los respaldos en correspondencia con los requisitos de la entidad, los requisitos de seguridad de la información implicada, y la importancia de la información que permita la operación continua de la organización;
d) precisar las copias que son almacenadas en un área apartada del lugar habitual de procesamiento de la información que se preserva, a una suficiente distancia para la salvaguarda de cualquier daño producto de un desastre en el sitio principal;
e) establecer un nivel apropiado de protección ambiental y físico (ver punto 6.3. “Seguridad Física y Ambiental”) de la información de respaldo, consistente con las normas aplicadas en el sitio principal; los controles aplicados a los soportes en el sitio principal se extienden para cubrir el sitio de respaldo;
f) probar regularmente los soportes de respaldo para verificar que puede confiarse en ellos para el uso cuando sean necesarios;
g) comprobar regularmente los procedimientos de restauración para asegurar que son eficaces y que pueden ser utilizados dentro del tiempo asignado en los procedimientos de recuperación; y
h) proteger los respaldos por medio del cifrado en los casos que se requiera.

Para los sistemas críticos, las disposiciones de respaldo cubren la información y datos para recuperar el sistema completo en caso de un desastre.

Los procedimientos de respaldo, cuando sea posible, se automatizan para facilitar el respaldo y los procesos de restauración. Tales soluciones automatizadas se prueban suficientemente, antes de la puesta en práctica y en intervalos regulares.

Ejemplo de un procedimiento de respaldo en la Empresa X

***Procedimiento 7* Respaldo de Aplicaciones.**

1. *Realizar diariamente la salva de:*
   a) *Sistema Contable (CONTAB).*
   b) *Sistema de Control de Información Clasificada (SCIC).*
   c) *Sistema de Control de componentes (Everest).*
   d) *Sistema de Control de Actualizaciones (WSUS).*
   e) *Sistema de Representación Geoespacial (SIRGE).*

   Al finalizar la jornada de trabajo en discos compactos en dos versiones. Una copia es guardada en el local del administrador de la red y la otra en la oficina de la secretaria del director.
   ***Responsable:** Administradores de sistemas*
2. *Verificar la integridad de la salva.*
   ***Responsable:** Administradores de sistemas*
3. *Consignar en el registro de salvas de aplicaciones (Registro 4) las acciones de respaldo realizadas*
   ***Responsable:** Administradores de sistemas*
4. *Realizar un control trimestral (incluyen revisión del registro), del cumplimiento de este procedimiento.*
   ***Responsable:** Jefe Departamento de Organización y Supervisión*

6.8. Seguridad en Redes

En esta parte del plan se incluyen las acciones a realizar para garantizar la seguridad de las redes y sus servicios, mediante la habilitación de las opciones de seguridad con que cuentan los sistemas operativos y de otras iniciativas dirigidas a lograr la seguridad de los servidores y terminales, el acceso a la información solamente por el personal autorizado y los elementos que permitan el monitoreo y auditoría de los principales eventos.

Se describe la configuración de los componentes de seguridad de las redes y servicios implementados y la instalación de los medios técnicos destinados a establecer una barrera de protección entre las tecnologías de la entidad y las redes externas. Para lo cual se tiene en cuenta:

1. Barreras de protección y su arquitectura.
2. Empleo de Cortafuegos, Sistemas Proxy y otros.
3. Filtrado de paquetes.
4. Herramientas de administración y monitoreo.
5. Habilitación de trazas y subsistemas de auditoría.
6. Establecimiento de alarmas del sistema.
7. Dispositivos de identificación y autenticación de usuarios.
8. Software especial de seguridad.
9. Medios técnicos de prevención y detección de intrusos (IPS/IDS).

Se especifican los procedimientos requeridos para el cumplimiento de las obligaciones de los administradores de redes en relación con la seguridad, en particular los relacionados con:

1. La aplicación de los mecanismos que implementan las políticas de seguridad aprobadas.
2. El análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red.
3. El análisis del empleo de los servicios de red implementados.
4. Las acciones de respuesta en caso de la ocurrencia de incidentes o actividades nocivas.

Se incluyen los procedimientos instrumentados para la verificación de la seguridad de las redes y la detección de vulnerabilidades.

Ejemplo de un procedimiento de auditoría de eventos del sistema operativo en la Empresa X

***Procedimiento 8* Auditoría de eventos del sistema operativo.**

1. *Realizar diariamente la revisión y análisis de los registros de los eventos generados por el sistema operativo de la red.*
2. *Investigar las causas de cualquier anomalía detectada y determinar si se está en presencia de un incidente de seguridad, actúa según lo establecido para esos casos.*
3. *Emplear, cuando se requiera, el software SAWMILL para la revisión de las trazas de auditoría.*
4. *Anotar las acciones realizadas y sus resultados en el registro de auditorías de eventos del S.O. (Registro 5).*
5. *Mantener la disponibilidad y actualización de las herramientas que garantizan la auditoría de los eventos del sistema operativo.*

Responsable: *Administrador de la red*

6. *Realizar una verificación trimestral del cumplimiento de este procedimiento.*
   Responsable: *Jefe Departamento de Informática*

6.9. Gestión de Incidentes de Seguridad

Se describen las medidas y procedimientos de detección, neutralización y recuperación ante cualquier eventualidad que pueda paralizar total o parcialmente la actividad informática o degraden su funcionamiento, minimizan el impacto negativo de éstas sobre la entidad.
Los incidentes de seguridad incluyen entre otros:

1. Acceso (intentos de acceso) no autorizado a un sistema o sus datos.
2. Interrupción no deseada o negación de servicio.
3. Uso no autorizado de un sistema para el procesamiento o almacenamiento de información.
4. Suplantación de identidad.
5. Cambios a las características del equipamiento, las aplicaciones o datos del sistema sin el conocimiento o consentimiento del responsable de dicho sistema.

Al producirse los incidentes es fundamental que existan los mecanismos para:

1. Detectar e identificar eficazmente el incidente.
2. Crear estrategias de mitigación y respuesta.
3. Establecer canales confiables de comunicación.
4. Proporcionar alertas tempranas a quien lo requiera.
5. Ofrecer una respuesta coordinada a los incidentes.

A partir de los resultados obtenidos en el análisis de riesgos, se determinan las acciones a realizar para neutralizar aquellas amenazas que tengan mayor probabilidad de ocurrencia en caso de materializarse, así como para la recuperación de los procesos, servicios o sistemas afectados, precisan en cada caso:

1. Qué acciones se realizan.
2. Quién las realiza.
3. Cómo se realizan.
4. De qué recursos se dispone.

Los procedimientos para la gestión de incidentes especifican los pasos a seguir para garantizar:

1. La correcta evaluación de lo ocurrido.
2. A quién, cómo y cuándo se reportan.
3. Los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial.

Se habilita un registro donde se consignan los incidentes que se produzcan en la entidad, que es conservado por un período no menor de cinco (5) años y es utilizado como criterio de medición para la gestión del sistema de seguridad informática.

Ejemplo de un procedimiento de gestión de incidentes en la Empresa X

***Procedimiento 9* Interrupción en las comunicaciones**

1. *Informar a la Dirección de la Empresa la situación que se ha presentado.*
2. *Identificar si la interrupción es causada por factores externos o internos.*
3. *Reportar la interrupción al proveedor del servicio si el problema radica en la línea de comunicación.*
4. *Restablecer la operación y establecer las causas de la interrupción y determinar posibles acciones para evitar su reiteración una vez solucionado el problema.*
5. *Anotar las acciones realizadas y sus resultados en el registro de incidencias. (Registro 6).*
6. *Reportar el incidente a la OSRI.*
   ***Responsable:** Administrador de la red*

7. Anexos del Plan de Seguridad Informática

7.1 Listado nominal de Usuarios con acceso a los servicios de red

Se habilita un listado de usuarios autorizados por cada servicio, especifican nombre, apellidos y cargo que ocupa en la entidad, así como los servicios para los que está autorizado.

7.2 Registros

Se definen los documentos de registro que se determinen a partir de los eventos y procedimientos que demanden dejar constancia, ya sea por requerimientos legales y de supervisión, con fines de análisis para elaborar tendencias o simplemente para el control de las actividades que se realizan, en correspondencia con las necesidades del SGSI implementado.

7.3 Control de Cambios

Se dispone de un modelo donde se registren aquellos cambios que motivan variaciones en el PSI y que por su magnitud no ameritan editar el plan en su totalidad nuevamente. Se incluyen los cambios que se realicen, la fecha, la parte del plan que se modifica, el nombre de la persona que autoriza la modificación y el de la persona que la realiza.

RESOLUCIÓN No. 128/2019

POR CUANTO: El Decreto 360 “Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional”, de 5 de junio de 2019 en su Disposición Final Primera establece, que los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización, y establecen las coordinaciones que resulten necesarias relativas a la aplicación del referido Decreto.

POR CUANTO: A partir de la experiencia acumulada en la aplicación de las resoluciones 127 del Ministro de la Informática y las Comunicaciones, que aprobó el Reglamento de Seguridad de las Tecnologías de la Información, del 24 de julio de 2007 y la 192, del 20 de marzo de 2014, del Ministro de Comunicaciones, que puso en vigor el Reglamento para contrarrestar el envío de mensajes masivos dañinos a través de las redes de telecomunicaciones; resulta necesario emitir una nueva disposición normativa que actualice el contenido normativo de las referidas disposiciones, para atemperarlas a las exigencias del proceso de informatización de la sociedad y en consecuencia proceder a su derogación.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. El presente Reglamento tiene por objeto complementar las disposiciones del Decreto 360 “Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional” de 5 de junio de 2019, y establecer las funciones de los sujetos que intervienen en esta, así como garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país.

Artículo 2. Este Reglamento es de aplicación a los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales, los órganos del Poder Popular, el sistema empresarial y las unidades presupuestadas, las formas de propiedad y gestión no estatal, las empresas mixtas, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas y las personas naturales, en lo adelante la entidad.

CAPÍTULO II
DEL SISTEMA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 3. El Sistema de Seguridad de las Tecnologías de la Información y la Comunicación tiene como objetivo minimizar los riesgos sobre los sistemas informáticos y garantizar la continuidad de los procesos informáticos.

Artículo 4. Las formas de propiedad y gestión no estatal y las personas naturales, cumplen lo dispuesto en el presente Reglamento, en lo que corresponda, aunque no cuenten con el personal especializado.

Artículo 5. El jefe de la entidad a cada nivel es el máximo responsable de la seguridad de las Tecnologías de la Información y la Comunicación, en lo adelante seguridad de las TIC, en su organización, y garantiza la actualización de los Planes de Seguridad de las TIC y considera para ello los factores siguientes:

a) La aparición de nuevas vulnerabilidades;
b) los efectos de los cambios de tecnología o de personal;
c) la efectividad del sistema, demostrada por la naturaleza, número y daño ocasionado por los incidentes de seguridad registrados.

Artículo 6. Los especialistas en seguridad de las TIC a cada nivel, cumplen las funciones siguientes:

a) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad de las TIC, supervisar su aplicación y disciplina en su cumplimiento;
b) establecer y mantener los controles, en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática diseñado;
c) participar en la evaluación de riesgos y vulnerabilidades de su entidad;
d) controlar y supervisar la disponibilidad de los bienes informáticos;
e) asesorar a las distintas instancias sobre los aspectos técnicos vinculados con la seguridad de las TIC;
f) establecer los controles necesarios para impedir la instalación de cualquier tipo de hardware o software, sin la autorización de la dirección de la entidad;
g) participar en la elaboración de los procedimientos de recuperación, ante incidentes de seguridad y en sus pruebas periódicas;
h) informar a los usuarios de las regulaciones establecidas.

Artículo 7. Los responsables de la seguridad de las TIC a cada nivel, responden por la protección de los bienes informáticos que le han sido asignados y tienen los deberes siguientes:

a) Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, determinar el nivel de acceso de los usuarios y la vigencia de estos accesos;

b) participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad de las TIC en la parte que concierne a su esfera de acción y garantizar su cumplimiento;
c) participar en la evaluación de riesgos y vulnerabilidades de su entidad;
d) aplicar las medidas y procedimientos establecidos en su área de responsabilidad;
e) especificar al personal subordinado, las medidas y procedimientos establecidos y controlar su cumplimiento;
f) participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas;
g) imponer o proponer sanciones ante violaciones del Sistema de Seguridad, en correspondencia con su naturaleza y con los daños ocasionados.

Artículo 8. Los usuarios de las TIC en sus entidades, tienen los deberes siguientes:

a) Adquirir la preparación necesaria y los conocimientos de Seguridad de las TIC imprescindibles para el desempeño de su trabajo;
b) contar con la autorización expresa del jefe facultado, para obtener acceso a cualquiera de los bienes informáticos;
c) cumplir las medidas de seguridad establecidas;
d) proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usar la información que contiene o utilizar de manera impropia el sistema al que esté conectado;
e) contar con la autorización del jefe facultado para instalar o utilizar en las tecnologías, equipamientos, o programas, o modificar su configuración;
f) cumplir las reglas establecidas para el empleo de las contraseñas;
g) informar al dirigente facultado de cualquier anomalía de seguridad detectada.

CAPÍTULO III
DEL EMPLEO SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Sección Primera
Bienes informáticos

Artículo 9. Los bienes informáticos están bajo la custodia documentada legalmente de la persona designada para hacer uso del bien, quien es responsable de su protección.

Artículo 10. El jefe de la entidad instrumenta los procedimientos que se requieran para garantizar la autorización y el control sobre la utilización y movimiento de los bienes informáticos.

Artículo 11. El jefe del área o unidad organizativa que atiende las TIC define el procedimiento de uso de empleo y responsabilidad de los bienes informáticos que son móviles (portátiles o removibles), para las personas que utilizan estos bienes dentro y fuera de la entidad, que incluye:

a) Comunicar de inmediato por el usuario a la dirección de la entidad la pérdida o extravío del bien;
b) no contener datos importantes e información sensible, cuando se extraigan de la entidad, y tener implementadas medidas de protección;
c) no conservar datos personales o sobre la entidad a través de los que se pueda acceder a sus sistemas.

Sección Segunda
De la Dirección del personal

Artículo 12. Las funciones y responsabilidades de seguridad de las TIC, tanto generales como específicas, son debidamente documentadas e incluidas dentro de las responsabilidades laborales del personal de la entidad.

Artículo 13. El jefe del área o unidad organizativa que atiende las TIC de la entidad está obligado a preparar y exigir responsabilidad al trabajador en materia de seguridad de las TIC, así como a aplicar las sanciones en caso de que este incumpla los requerimientos establecidos.

Artículo 14. La dirección de cada entidad establece previamente la utilización de las TIC y sus servicios asociados conforme a la necesidad de uso en interés de la propia entidad.

Artículo 15. La introducción, ejecución, distribución o conservación de programas en los medios de cómputo que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad, sólo se efectúan por las personas debidamente autorizadas por el jefe del área o unidad organizativa que atiende las TIC; se excluye el uso de aplicaciones destinadas a la comprobación de los sistemas instalados en la organización para el control interno de las operaciones realizadas y en ningún caso, este tipo de programas o información se expone mediante las TIC para su libre acceso.

Sección Tercera
Seguridad Física

Artículo 16. En los edificios e instalaciones de cada entidad, su dirección determina las áreas o zonas controladas con requerimientos específicos, protegidas por un perímetro de seguridad definido, en dependencia de la importancia de los bienes informáticos que contiene y su utilización de acuerdo con la denominación siguiente:

a) **Áreas limitadas:** en las que se concentran bienes informáticos de valor medio, cuya afectación puede determinar parcialmente los resultados de la gestión de la entidad o de terceros.
b) **Áreas restringidas:** donde se concentran bienes informáticos de alto valor e importancia crítica, cuya afectación pueda paralizar o afectar severamente la gestión de sectores de la economía o de la sociedad; territorios o entidades.
c) **Áreas estratégicas:** en las cuales se concentran bienes informáticos de alto valor e importancia crítica, que inciden de forma determinante en la seguridad y la defensa nacional; la seguridad aeronáutica; biológica; industrial; la generación y distribución de energía eléctrica; las redes informáticas y de comunicaciones del país; las relaciones exteriores y de colaboración; la

economía nacional; las investigaciones científicas y el desarrollo tecnológico; la alimentación de la población; la salud pública, y el suministro de agua u otra que por su importancia se considere necesaria.

Artículo 17. Las áreas o zonas controladas se protegen para garantizar el acceso exclusivamente al personal autorizado y la dirección de la entidad establece las medidas que correspondan.

Artículo 18. En la selección y diseño de las áreas controladas se tiene en cuenta la posibilidad de daño por fuego, inundación, explosión, perturbaciones del orden y otras formas de desastre natural o artificial.

Artículo 19. El equipamiento instalado en las áreas controladas se protege contra fallas de alimentación y otras anomalías eléctricas, lo que incluye el uso de fuentes de alimentación alternativas para los procesos que deben continuar en caso de un fallo de electricidad prolongado, así como se ubica y protege de manera tal que se reduzcan los riesgos de amenazas ambientales y oportunidades de cualquier tipo de acceso no autorizado.

Artículo 20. En las áreas limitadas se aplican las medidas de protección física siguientes:

a) Seleccionar para su ubicación locales cuyas puertas y ventanas estén provistas de cierres seguros;
b) aplicar medidas que garanticen su seguridad y eviten la visibilidad hacia el interior de los locales con ventanas que se comuniquen al exterior de la instalación;
c) prohibir el acceso de personal no autorizado por la dirección de la entidad;
d) permitir la permanencia del personal fuera del horario laboral con la debida justificación y autorización por escrito de la dirección de la entidad; las autorizaciones referidas se conservan por un término mínimo de seis meses.

Artículo 21. En las áreas restringidas además de las medidas requeridas en las áreas limitadas, se aplican las siguientes:

a) Se mantienen cerradas incluso cuando permanezcan personas laborando, y el acceso se controla mediante los registros que para ello se establezcan;
b) establecer por la entidad requisitos de idoneidad, al personal que accede a estas áreas;
c) utilizar sistemas de detección y alarma que permitan una respuesta efectiva ante accesos no autorizados, cuando no se encuentre el personal que en ellas labora;
d) implementar mecanismos y procedimientos de supervisión de la actividad que se realiza en estas áreas;
e) prohibir la introducción de soportes ópticos y magnéticos personales, excepto los que hayan sido autorizados de forma expresa por la dirección de la entidad; así como de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a esta.

Artículo 22. En las áreas estratégicas además de las medidas requeridas en las áreas restringidas y limitadas, se aplican las siguientes:

a) Establecer una identificación individual que especifique las áreas de trabajo para el personal que labore o que por razones de servicio sea autorizado a permanecer en estas; la cual debe llevarse por cada trabajador en un lugar visible;
b) implementar medios especiales de supervisión de la actividad que en ellas se realiza;
c) el acceso por personas ajenas solo se autoriza de manera excepcional, restringida y bajo supervisión, mediante un permiso especial, emitido por la dirección de la entidad, el que se conserva por un término mínimo de seis meses.

Artículo 23. Los recursos relacionados con las TIC, independientemente de su importancia, se protegen contra alteraciones o sustracciones, ya sea de éstas, de sus componentes o de la información que contienen.

Artículo 24. El jefe de la entidad es el responsable de que el equipamiento reciba el mantenimiento correcto de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante, con el fin de asegurar su disponibilidad e integridad; en caso de necesidad de envío del equipamiento fuera de las instalaciones para que reciban mantenimiento, este se realiza en correspondencia con los procedimientos establecidos por la dirección de la entidad a tales efectos, según las regulaciones vigentes en el país en materia de protección de la información.

Artículo 25. El uso fuera de las instalaciones de una entidad de cualquier equipo para el procesamiento de información se autoriza por su dirección, mediante el documento correspondiente; la seguridad que se le garantice por el autorizado tiene que ser equivalente a la establecida en las instalaciones habituales del equipamiento usado para este propósito.

Artículo 26. El equipamiento antes de causar baja o ser destinado a otras funciones, se le aplica el procedimiento de borrado seguro, para evitar que la información que contiene pueda resultar comprometida; los dispositivos de almacenamiento que contengan información crítica para la entidad son destruidos físicamente.

Artículo 27. Se prohíbe el movimiento de los equipos de la entidad y de los programas y aplicaciones informáticas sin la autorización escrita del jefe facultado; en caso de que se autorice se registra el movimiento a la salida del medio y a su entrada al reintegrarse a su origen; así como se realizan los controles sorpresivos para detectar las extracciones no autorizadas.

CAPÍTULO IV
SEGURIDAD DE LAS OPERACIONES

Artículo 28. Las acciones para cubrir las brechas de seguridad y la corrección de los errores de los sistemas y aplicaciones son minuciosamente controladas en cada entidad, por sus respectivos jefes; los procedimientos aseguran en lo fundamental que:

a) Sean eliminadas o minimizadas las vulnerabilidades conocidas;
b) solo el personal identificado y autorizado tenga acceso a sistemas en funcionamiento y a los datos;

c) todas las acciones de emergencia tomadas sean documentadas detalladamente;
d) la acción de emergencia sea reportada a la dirección de la entidad y realizada de manera ordenada.

Artículo 29. En caso de ser necesario compartir recursos a través de la red, se define, por la persona autorizada, de forma precisa con los usuarios se hará, el nivel de acceso y la duración del intercambio.

Artículo 30. En el uso de credenciales de acceso, cuya contraseña es textual, como método de autenticación de usuarios, se cumplen los requisitos siguientes:

a) Ser privadas e intransferibles;
b) su estructura, fortaleza y frecuencia de cambio se corresponden con el riesgo estimado para el acceso que protegen, implementado a través de mecanismos automatizados de validación;
c) la composición de los caracteres es alfanumérica (letras, números y símbolos) sin un significado trivial, con una longitud mínima de 8 caracteres;
d) no pueden ser visualizadas en pantalla mientras se teclean;
e) no se almacenan en texto claro, sin cifrar, ni son recordadas en ningún tipo de terminal.

Artículo 31. En el caso de mecanismos de autenticación diferentes al mencionado anteriormente, se cumple las normas de seguridad establecidas para estos.

Artículo 32. El jefe de la entidad aprueba los derechos y privilegios de acceso a sistemas y datos que tiene cada usuario, así como el procedimiento escrito en cada caso para otorgar o suspender estos accesos.

Artículo 33. Ante indicios de contaminación por programas malignos, tanto en redes como en equipos no conectados a redes, se procede al cese de la operación de los medios implicados y a su desconexión de las redes cuando corresponda, y se preserva para su posterior análisis y descontaminación por personal especializado; además, se revisan los soportes con los que haya interactuado el medio contaminado.

Artículo 34. La contaminación por programas malignos se considera un incidente de seguridad y se cumple en este caso lo establecido en el Artículo 48 del presente Reglamento; en todos los casos se tiene que determinar el origen y la responsabilidad de las personas involucradas.

Artículo 35. El usuario que a través de sus equipos terminales de telecomunicaciones reciba mensajes masivos dañinos, tiene el derecho de presentar a su operador o proveedor una queja con las pruebas relativas de los hechos ocurridos; al que le corresponde tomar las medidas que procedan para eliminar la situación surgida.

CAPÍTULO V
SEGURIDAD DE LAS REDES

Artículo 36. El administrador de una red informática tiene, en relación con la seguridad de las TIC, los deberes siguientes:

a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red;
b) realizar el análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red;
c) garantizar que los servicios implementados sean utilizados para los fines que fueron creados;
d) comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes;
e) activar los mecanismos técnicos y organizativos de respuesta ante distintos tipos de incidentes y acciones nocivas que se identifiquen, y preservar toda la información requerida para su esclarecimiento;
f) participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas;
g) informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento;
h) garantizar que en el registro de trazas se incluya las relacionadas con la navegación a Internet, que permitan correlacionar la dirección IP real de salida al proveedor de servicios de Internet, con las IP privadas empleadas en las redes internas de la entidad;
i) participar en la confección y actualización del Plan de Seguridad de las TIC;
j) implementar y operar los controles que se establezcan para gestionar los riesgos de seguridad.

Artículo 37. En el empleo de las redes inalámbricas se tienen en cuenta, además de los aspectos de su seguridad, los siguientes:

a) Contar con la autorización, a través del procedimiento establecido, de la entidad facultada para su despliegue y explotación;
b) utilizar protocolos de cifrado de datos aprobados para la red de telecomunicaciones inalámbrica que lo requiera;
c) utilizar filtrado de direcciones MAC (conocida como Media Access Control) cuando sea posible y no se afecten los servicios para la que están destinadas;
d) configurar la potencia de irradiación al nivel establecido por la autoridad facultada a esos efectos.

Artículo 38. El jefe de la entidad orienta la ejecución de procedimientos periódicos de verificación de la seguridad de las redes, con el fin de detectar posibles vulnerabilidades, incluye para ello, cuando sea procedente, la comprobación de forma remota por entidades facultadas oficialmente, debido a la sensibilidad de estas acciones.

Artículo 39. En las redes donde se establezcan servicios de intercambio de datos o mensajes con otras redes o usuarios externos, se implementan mecanismos de seguridad que garanticen la confidencialidad, la integridad, el control de accesos, la autenticación y el no repudio, según corresponda.

Artículo 40. En los casos de redes corporativas que prevean la extrapolación de servicios internos, la conexión se realiza por puertos bien identificados y mediante la protección con dispositivos que garanticen el acceso a esos servicios por el personal autorizado.

Artículo 41. Los servicios que ofrecen las redes de datos de una entidad mediante conexiones externas, solo se utilizan en interés de esta; la asignación de cuentas para su empleo se aprueba, en todos los casos, por la dirección de la entidad, sobre la base de las necesidades requeridas para su funcionamiento.

Artículo 42. Los servicios ofrecidos al público que son autorizados a una entidad específica, no forman parte de la red corporativa.

Artículo 43. La configuración del servicio de correo electrónico tiene que garantizar que solo el propietario de una cuenta pueda enviar y recibir mensajes desde esta.

Artículo 44. Se prohíbe vincular cuentas de correo electrónico de un servidor de una entidad a un servidor en el exterior del país, con el fin de redireccionar y acceder a los mensajes a través de este.

CAPÍTULO VI
DE LOS INCIDENTES DE SEGURIDAD

Artículo 45. La estrategia que se formule en la entidad ante cualquier incidente o violación de la seguridad es consecuente con sus objetivos básicos, donde se define el Plan de Prevención de Riesgos; además tiene en consideración:

a) Los riesgos que enfrenta en términos de probabilidad y su impacto, incluye una identificación y asignación de prioridades a los procesos críticos;
b) el impacto probable de las interrupciones sobre la gestión de la entidad;
c) la comprobación y actualización de manera periódica de los planes y procesos establecidos;
d) las acciones para la recuperación.

Artículo 46. Los procedimientos para la gestión de incidentes y violaciones de seguridad de las TIC, tienen los requisitos siguientes:

a) El reporte inmediato de la acción a la autoridad correspondiente;
b) la comunicación con los afectados o los involucrados en la recuperación del incidente;
c) el análisis y la identificación de las causas;
d) el registro de todos los eventos vinculados;
e) la recolección y preservación de las trazas de auditoría y otras evidencias;

f) la planificación y la implementación de medidas para prevenir la recurrencia, si fuera necesario.

Artículo 47. Ante cualquier incidente que afecte la seguridad de las TIC de una entidad, su dirección designa una comisión, integrada por especialistas no comprometidos directamente con este el hecho, encargada de realizar las investigaciones necesarias para esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

Artículo 48. La dirección de cada entidad queda obligada, al producirse un incidente o violación de la seguridad informática, reportarlo inmediatamente a la Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones y a la instancia superior de la entidad; este reporte incluye:

a) En qué consistió el incidente o violación;
b) fecha y hora de comienzo del incidente y de su detección;
c) implicaciones y daños para la entidad y para terceros;
d) acciones iniciales tomadas;
e) evaluación preliminar.

CAPÍTULO VII
PRESTACIÓN DE SERVICIOS DE SEGURIDAD INFORMÁTICA A TERCEROS

Artículo 49. La Dirección General de Informática del Ministerio de Comunicaciones es la unidad organizativa que autoriza las entidades que pueden brindar servicios de seguridad informática a terceros.

Artículo 50. Los requerimientos que cumple la entidad para solicitar la autorización que le permita prestar servicios de seguridad de las TIC a terceros, son los siguientes:

a) Que su objeto social se relacione con los servicios de las TIC;
b) que cuente con mecanismos que garanticen la calidad de los servicios y la idoneidad del personal;
c) preparación técnico-profesional de los especialistas que laboren en la entidad;
d) que esté en condiciones de cumplir los reglamentos y disposiciones establecidos en esta materia;
e) que cuente con medios de protección de la información a la que tenga acceso durante su trabajo;
f) que los productos de seguridad informática utilizados, estén debidamente autorizados por las entidades facultadas;
g) que sea una entidad estatal cuyo personal resida de forma permanente en el país.

Artículo 51. Las entidades autorizadas por la Dirección General de Informática para brindar servicios de seguridad informática en las redes de otras entidades, están en la obligación de:

a) Mantener el máximo de discreción en relación con las posibles vulnerabilidades detectadas;
b) abstenerse de la utilización del conocimiento obtenido sobre la red comprobada en beneficio propio;

c) informar a las entidades designadas para el control del ciberespacio, los resultados de las comprobaciones realizadas.

CAPÍTULO VIII
DE LA INSPECCIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 52. La inspección estatal a la seguridad de las TIC tiene como objetivos principales, los siguientes:

a) Evaluar los conocimientos y la aplicación de la base legal vigente;
b) realizar diagnósticos sobre la efectividad de los sistemas de seguridad informática aplicados en las entidades;
c) verificar el grado de control y supervisión que se ejerce sobre los bienes informáticos, así como los resultados de la gestión de la seguridad informática;
d) evaluar la efectividad de los planes de seguridad informática elaborados y su actualización y correspondencia con las necesidades de cada entidad;
e) valorar la gestión e influencia que ejercen las instancias superiores sobre esta actividad.

Artículo 53. Los inspectores de seguridad de las TIC tienen las facultades siguientes:

a) Realizar la inspección con o sin aviso previo;
b) evaluar el estado de cumplimiento y aplicación de la base legal de la Seguridad Informática vigente;
c) identificar las violaciones y vulnerabilidades detectadas en el Sistema de Seguridad Informática;
d) hacer evaluaciones, recomendaciones y disponer acciones correctivas ante violaciones de la base legal establecida;
e) proponer sanciones administrativas según las previstas en el Decreto 360 “Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional”;
f) recomendar la realización de auditorías;
g) proponer la suspensión de los servicios, cuando se viole lo establecido en el presente Reglamento;
h) verificar el cumplimiento de las acciones correctivas que hayan sido aplicadas como resultado de inspecciones anteriores, si las hubiere;
i) exigir la entrega de las trazas o registros de auditoría de las TIC u otras posibles evidencias que se consideren necesarias;
j) ocupar para su revisión los medios informáticos involucrados en cualquier tipo de incidente de seguridad y proponer su decomiso definitivo a las instancias correspondientes.

DISPOSICIÓN ESPECIAL

ÚNICA: Se facultan a los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, a adecuar para sus sistemas lo dispuesto en la presente Resolución.

DISPOSICIONES FINALES

PRIMERA: Se faculta al Director General de la Oficina de Seguridad las Redes Informáticas perteneciente a este Ministerio, para implementar las acciones que se requieran con el fin de dar cumplimiento a lo que por la presente se dispone.

SEGUNDA: El viceministro que atiende la Informática en el Ministerio de las Comunicaciones, instrumenta las medidas que se requieran en el control de los parámetros que sean necesarios para la contención de los mensajes masivos dañinos.

TERCERA: Derogar las resoluciones 127 del Ministro de la Informática y las Comunicaciones, del 24 de julio de 2007 y la 192 del Ministro de Comunicaciones, del 20 de marzo de 2014.

NOTIFÍQUESE a los directores generales de Defensa y de la Oficina de Seguridad para las Redes Informáticas, a los directores territoriales de control, todos del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, al director general de Informática y al director de Regulaciones, del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella

RESOLUCIÓN No. 126/2019

POR CUANTO: El Acuerdo 8151, del 22 de mayo de 2017, del Consejo de Ministros, en sus numerales Tercero, Duodécimo y Decimonoveno del Apartado Primero, establece que el Ministerio de Comunicaciones es el organismo encargado de proponer, y una vez aprobada, ejecutar y controlar la política sobre el uso del ciberespacio, así como planificar, implementar, reglamentar, administrar y controlar el sistema de medidas necesarias para su defensa; regular y controlar la aplicación de las

normas técnicas y operacionales de los sistemas de comunicaciones y las redes informáticas en general que funcionan en el país, encaminadas al desarrollo tecnológico; y autorizar la asignación de los recursos de numeración, de Internet y de uso conjunto a los operadores de servicios público de telecomunicaciones.

POR CUANTO: La Resolución del de 2019, del Ministro de Comunicaciones, que aprobó el Reglamento de Seguridad de las Tecnologías de la Información y la Comunicación establece que en las redes informáticas se tienen que implementar mecanismos de seguridad, que garanticen su protección, por lo que procede disponer de un conjunto de medidas de control, que incluye los tipos de herramientas de seguridad que operan en las redes privadas de datos del país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el presente Reglamento que establece las medidas de control y los tipos de herramientas de seguridad que se implementan en las redes privadas de datos, inscritas en el Control Administrativo Central Interno del Ministerio de Comunicaciones.

SEGUNDO: Los titulares o los jefes administrativos de redes privadas de datos son los responsables de la implementación en sus redes de las medidas de control y los tipos de herramientas de seguridad que por la presente se establecen y de que estas sean de código abierto, preferentemente.

TERCERO: La Dirección de Control de acceso al medio, por sus siglas en inglés MAC, es la dirección física, única de cada dispositivo de red y herramienta de seguridad al dispositivo de hardware o software diseñado para proporcionar o comprobar la seguridad en un sistema informático.

CUARTO: Las medidas de control que se establecen son las siguientes:

a) Monitoreo físico e inspección visual al sistema de red, con registros trimestrales;
b) registros actualizados de infraestructura: cableado, enrutadores, conmutadores, terminales, servidores y puntos de acceso, AP de redes inalámbricas;
c) barreras de protección entre las tecnologías de la información y la comunicación que brindan servicios al interior de la red y las redes externas a estas;
d) procedimiento donde se regula el sistema para el uso de las contraseñas de usuarios y dispositivos de la red, la autenticación de usuarios, denominación de equipos y el direccionamiento IP, tiene en cuenta que en las redes inalámbricas no sea dinámico, la deshabilitación de protocolos innecesarios en los enrutadores, la desconexión de los AP sin uso, la activación del filtrado por direcciones MAC, y la encriptación en la configuración de la conexión que lo requiera, así como la legislación vigente sobre este tema;
e) procedimiento donde se definen los tipos de sistemas de supervisión, control, detección y alarma que permiten reaccionar proactivamente y dar una respuesta efectiva ante amenazas de ciberseguridad;

f) procedimiento para que los administradores de redes puedan proponer herramientas complementarias y exista un mecanismo de autorización para incorporarlas;
g) crear un repositorio interno y su sistema de salvas que permita aplicar la gestión de las actualizaciones de seguridad;
h) la gestión de las trazas de los servicios y sistemas informáticos;
i) la implementación de la revisión de los sistemas y servicios que se instalen o empleen.

QUINTO: Las herramientas de seguridad, de las cuales se brinda información sobre sus funciones en el anexo que es parte integrante de la presente Resolución, cumplen los objetivos siguientes:

a) Mostrar el estado actualizado de los servicios implementados en cada servidor;
b) supervisar la carga y disponibilidad de los servidores;
c) establecer un Sistema de Detección y Prevención de Intrusos, por sus siglas en inglés IDS/IPS;
d) monitorear el comportamiento del tráfico de la red, análisis de protocolos y detección de anomalías;
e) dar seguimiento a las trazas;
f) detectar posibles vulnerabilidades en la red;
g) controlar centralizadamente el estado físico del hardware y del software;
h) gestionarlas actualizaciones de seguridad;
i) establecer un sistema de correlación de eventos;
j) realizar el aviso oportuno ante la detección de anomalías o eventos de ciberseguridad.

SEXTO: El empleo de los medios de control y herramientas de seguridad permite:

a) La planificación de su expansión y el perfeccionamiento de la prestación de sus servicios;
b) la detección de fallos e incidentes y su investigación;
c) la ejecución de las pruebas, de acuerdo con lo establecido;
d) el desarrollo de las auditorías informáticas internas o externas, que se ejecuten.

SÉPTIMO: En computadoras o servidores habilitados se instalan barreras y otros medios de protección y se incorporan herramientas de seguridad que permitan el control y monitoreo de los servidores, servicios y usuarios de la red.

OCTAVO: En las computadoras o servidores que constituyen la subred de las terminales de los usuarios de acuerdo al rango IP y nivel de cliente y la subred de los servidores según rango IP y nivel de servidor, se instalan las herramientas que propicien las barreras de protección a los efectos de aplicar políticas convenientes para la aceptación y denegación de tráfico de paquetes.

NOVENO: Las direcciones generales de Defensa, Informática y Comunicaciones, la Dirección de Inspección, la Oficina de Seguridad de las Redes Informáticas y las oficinas territoriales de control, quedan encargadas del control y fiscalización, en lo que a cada cual le corresponda, así como la implementación de las medidas que se requieran para garantizar el cumplimiento de lo dispuesto en la presente Resolución.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministerios de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas, las medidas de control y los tipos de herramientas de seguridad que se implementan en las redes privadas.

DESE CUENTA a los jefes de los órganos y organismos de la Administración Central del Estado y de entidades nacionales.

NOTIFÍQUESE a los directores generales de Defensa, Informática, Comunicaciones y de la Oficina de Seguridad para las Redes Informáticas, al director de Inspección y a los directores territoriales de control del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros y al director de Regulaciones del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 del mes de junio del 2019

Jorge Luis Perdomo Di-Lella

5. CALIDAD Y AHORRO

RESOLUCIÓN No. 124/2019

POR CUANTO: El Decreto 359 “Sobre el desarrollo de la Industria de Programas y Aplicaciones Informáticas” de 5 de junio de 2019, en su Disposición Final Primera establece que los jefes de los órganos y organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular que correspondan, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización, y establecen las coordinaciones que resulten necesarias relativos a la aplicación de este Decreto.

POR CUANTO: En el proceso de reordenamiento de la industria nacional del software se requiere garantizar la calidad de los programas y aplicaciones informáticos que se desarrollan y comercializan en el país; para alcanzar estos objetivos, es necesario establecer el Reglamento con las acciones a realizar por las personas que desarrollan y comercializan programas y aplicaciones informáticas, disponer las reglas básicas que normen su producción y la evaluación de la calidad de estos procesos productivos y de sus productos resultantes.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO PARA LA PRODUCCIÓN DE LOS PROGRAMAS Y APLICACIONES INFORMÁTICAS Y LA EVALUACIÓN DE SU CALIDAD

CAPÍTULO I
OBJETO, DEFINICIONES Y GENERALIDADES

Artículo 1. El objeto del presente Reglamento es establecer:

a) Las reglas básicas para la producción de programas y aplicaciones informáticas;
b) la evaluación del proceso de desarrollo de la producción de programas y aplicaciones informáticas;
c) el proceso para la evaluación de la calidad por un tercero de los programas y aplicaciones informáticas.

Artículo 2. El presente Reglamento no incluye la evaluación a los programas y aplicaciones informáticas que constituyan un software empotrado en el equipamiento.

Artículo 3. Este Reglamento es de aplicación a los desarrolladores de programas y aplicaciones informáticas, en lo adelante el desarrollador, a los comercializadores y a los evaluadores autorizados.

Artículo 4. La evaluación de los productos puede ser solicitada por un cliente, por iniciativa del desarrollador o comercializador, cuando se destine a la exportación o se determine por la Dirección General de Informática del Ministerio de Comunicaciones.

Artículo 5. Se autoriza al Centro Nacional de Calidad del Software, en lo adelante Calisoft, como proveedor de servicio público de evaluación de procesos y de programas y aplicaciones informáticas.

CAPÍTULO II
DE LA EVALUACIÓN DE PROCESO

Artículo 6. Los desarrolladores tienen que implementar las reglas básicas para la producción de programas y aplicaciones informáticas, que se relacionan en el Anexo 1 que forma parte integrante de la presente Resolución, y poseer evidencia de su cumplimiento por cada proyecto que ejecute.

Artículo 7.1. La evaluación del proceso de desarrollo se solicita al evaluador autorizado para la validación de la implementación de las reglas básicas; el desarrollador al solicitar la evaluación del proceso entrega sus datos generales o los de la entidad y la evidencia del cumplimiento de las referidas reglas de los proyectos seleccionados.

2. Los documentos a entregar, el procedimiento de evaluación y los resultados de esta, se publican y actualizan en el sitio Web del evaluador autorizado.

Artículo 8. El evaluador autorizado no puede divulgar la información entregada para la evaluación de proceso, ni los datos generados de estas, y garantizan su confidencialidad.

Artículo 9. Los desarrolladores que están certificados con normas nacionales o internacionales para validar la implementación de las reglas básicas para la producción de programas y aplicaciones informáticas, entregan evidencia de la certificación a la Dirección General de Informática y esta evalúa si la norma por la que está certificado, cumple con las reglas básicas; la Dirección General de Informática publica el desarrollador que cumple los requisitos en el sitio Web del Ministerio de Comunicaciones.

CAPÍTULO III
DE LA EVALUACIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

Artículo 10. La evaluación de las características de la calidad de programas y aplicaciones informáticas incluye pruebas de usabilidad, adecuación funcional, eficiencia de desempeño, fiabilidad, portabilidad y de seguridad, esta última de acuerdo con la protección de la información y los datos que contiene, evita que otros productos o sistemas tengan capacidad de acceso a los datos según sus tipos y niveles de autorización; la prueba antes mencionada no exime de la realización de la otra evaluación de seguridad establecida por la legislación vigente; el evaluador autorizado publica en su sitio Web las reglas y métricas de las pruebas.

Artículo 11. Al desarrollador y comercializador, que por su naturaleza, destino u otra razón fundamentada sobre su programa y aplicación informática, se le solicita la evaluación de la calidad por la Dirección General de Informática, está obligado a someterlos a la evaluación de la conformidad del evaluador autorizado, o presentar la documentación realizada por un evaluador internacional reconocido en el país.

Artículo 12. Los desarrolladores y comercializadores de productos nacionales o importados y cualquier persona interesada en adquirir un programa y aplicación informática, al solicitar al evaluador autorizado el dictamen técnico sobre la evaluación de la conformidad del producto desarrollado o comercializado, tienen que entregar lo siguiente:

a) El programa o aplicación desarrollada y el paquete de instalación o en su caso el programa de prueba, conocido como demo;
b) especificación de requisitos o funcionalidades;
c) pautas de diseño gráfico, en caso que se requiera;
d) documento con las consultas de la base de datos, si corresponde;
e) manual de usuario;
f) manual o guía de instalación y configuración, si es instalable por el usuario;
g) especificación del entorno donde se usa;
h) diseños de casos de prueba y juegos de datos, en caso que se requiera;

i) especificación de casos de uso o historias de usuario u otro documento técnico que permita detallar los requisitos, cuando se requiera;
j) documento de arquitectura de programa y aplicación informática, cuando corresponda;
k) arquitectura de información, si se requiere
l) certificación emitida por evaluadores internacionales referentes a los procesos y metodologías empleadas en el desarrollo de programas y aplicaciones informáticas, cuando lo posea;
m) otros que el evaluador autorizado establezca.

Artículo 13. El solicitante presenta al evaluador autorizado la información establecida en el artículo anterior en formato digital, y acompañado de documento que certifica la autenticidad y veracidad de la información, firmada por el jefe de su entidad, o por el interesado, si es una persona natural; el evaluador autorizado puede establecer las particularidades de la entrega, en dependencia del tipo de producto a evaluar, así como mecanismos de entrega en plataformas y servicios de red mediante procedimiento público y actualizado en su sitio web.

Artículo 14. El evaluador autorizado tiene hasta cinco días hábiles para revisar la información presentada y comunicar al solicitante si se le acepta esta o si debe modificarla o completarla.

Artículo 15. La evaluación de la conformidad de un programa y aplicación informática desarrollado o comercializado, tiene una validez de cinco años; decursado este período el producto requiere ser evaluado nuevamente.

Artículo 16.1. En la solicitud de la evaluación de conformidad que se realice, los desarrolladores o el comercializador de un programa y aplicación informática de desarrollo nacional presentan el resultado de la evaluación del proceso de producción de los desarrolladores.

2. Se exceptúa de la presentación del resultado de la evaluación del proceso de producción de los desarrolladores cuando la solicitud la promueva una persona interesada en adquirirlo.

Artículo 17. El evaluador autorizado no puede divulgar la información entregada para la evaluación de los programas y aplicaciones informáticas, ni los datos generados en estas, y acuerda en el contrato suscrito el tratamiento a los productos evaluados con garantía de su confidencialidad, de forma que no viole el derecho de autor sobre estos, en correspondencia con la legislación vigente en la materia.

Artículo 18. En la entrega de los datos considerados como información oficial clasificada, el cliente del servicio de evaluación cumple la legislación vigente en la materia.

Artículo 19.1. El evaluador autorizado, a partir de la información entregada por el solicitante, para realizar la validación correspondiente, tiene que cumplir lo siguiente:

a) Emitir el dictamen técnico sobre la evaluación de la conformidad del programa y aplicación informática desarrollado o comercializado, en un plazo de hasta sesenta días a partir de la notificación al solicitante de la fecha en que comienza el proceso de pruebas o informarle en caso de que no se puede dictaminar y explicar las razones;

b) inscribir el programa o aplicación desarrollada que haya recibido un dictamen técnico favorable en su base de datos de productos evaluados.

2. Los programas y aplicaciones informáticas notificadas con dictamen desfavorable, pueden ser presentados nuevamente cuando se rectifiquen los señalamientos realizados.

CAPÍTULO IV
SOBRE EL EVALUADOR

Artículo 20. El evaluador autorizado es el encargado de la divulgación y actualización en su sitio web de:

a) La documentación necesaria para el solicitante como parte del procedimiento de evaluación: solicitud del servicio, requisitos del servicio y criterios de evaluación;
b) la información que entregan los solicitantes para la evaluación de los procesos productivos y su procedimiento de evaluación;
c) la información que entregan los solicitantes para cada evaluación de los programas y aplicaciones informáticas y su procedimiento con particularidades;
d) los requisitos de calidad y las reglas y métricas con los que son evaluados los programas y aplicaciones informáticas;
e) la información de su base de datos de programas y aplicaciones informáticas validados favorablemente muestra la información general siguiente:
   I. relación de los programas y aplicaciones Informáticas inscritas, sus denominaciones, descripción y versiones;
   II. fecha de evaluación y características evaluadas al programa y aplicación informática;
   III. datos de los titulares de los programas y aplicaciones informáticas inscritos en su base de datos, así como de sus desarrolladores o comercializadores, según corresponda, que incluyen su sitio Web;
f) la información de su base de datos de evaluación de los procesos productivos validados favorablemente, muestra la información general siguiente:
   I. relación de los desarrolladores que han alcanzado el cumplimiento de las reglas básicas;
   II. fecha de evaluación.

Artículo 21. El evaluador autorizado brinda, previa solicitud, una información acordada con los titulares, más completa y detallada de los programas y aplicaciones informáticas inscritas en su base de datos.

Artículo 22. Los resultados de las evaluaciones realizadas por el evaluador autorizado son informados a la Dirección General de Informática.

SEGUNDO: La Dirección General de Informática es la encargada de divulgar y actualizar en el sitio web del Ministerio de Comunicaciones los evaluadores nacionales autorizados, y de diferenciar si se autoriza para la evaluación de procesos o de productos o para ambos.

TERCERO: La no presentación de los resultados de la evaluación del proceso de desarrollo o de la evidencia del cumplimiento de las reglas básicas establecidas en el Anexo 1 de la presente Resolución, es razón invalidante para la solicitud de la evaluación de programas y aplicaciones informáticas de producción nacional, según el plazo dispuesto en la Disposición Final Segunda.

DISPOSICIÓN ESPECIAL

ÚNICA: Los ministros de las Fuerzas Armadas Revolucionarias y del Interior, adecuan y regulan, de conformidad con las estructuras y particularidades de estas, la producción y evaluación de programas y aplicaciones informáticas propias para uso en sus sistemas.

DISPOSICIÓN TRANSITORIA

ÚNICA: Encargar al Director General de Informática del Ministerio de Comunicaciones de proponer al que resuelve, en el término de un año, a partir de la puesta en vigor de la presente Resolución, la aprobación del procedimiento y requisitos para la autorización de proveedores de servicio público de evaluación de procesos y de programas y aplicaciones informáticas.

DISPOSICIONES FINALES

PRIMERA: Los desarrolladores tienen un plazo de hasta un año, a partir de la entrada en vigor de la presente Resolución, para establecer en la producción de programas y aplicaciones informáticas, las reglas básicas, y después de este término solicitar la evaluación del proceso productivo.

SEGUNDA: El evaluador autorizado, a partir del plazo de dos años de la entrada en vigor de la presente Resolución, solicita como información obligatoria, la evaluación de proceso productivo del desarrollador, para poder realizar la evaluación de programas y aplicaciones informáticas.

TERCERA: Los directores de la Dirección General de Informática, la Dirección de Inspección y los jefes las oficinas territoriales de control, del Ministerio de Comunicaciones, y el evaluador autorizado, quedan encargados de controlar el cumplimiento de lo que por la presente se dispone, según corresponda.

CUARTA: El Director General de Calisoft queda responsabilizado con la aprobación de los procedimientos internos para la implementación de lo dispuesto en la presente Resolución a partir de su entrada en vigor.

QUINTA: El glosario de términos y definiciones del Anexo 2 forma parte del contenido de la presente Resolución.

NOTIFÍQUESE a los directores generales de Informática y Calisoft y a los directores territoriales de control, pertenecientes al Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones y de la Oficina de Seguridad para las Redes Informáticas, a los directores de Regulación e Inspección pertenecientes a este Ministerio.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 días del mes de junio del 2019.

Jorge Luis Perdomo Di-Lella

ANEXO 1

REGLAS BÁSICAS PARA LA PRODUCCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

1.- EN LA GESTIÓN ORGANIZACIONAL

1.1 Determinar los procesos

Implantar y describir los procesos utilizados para el desarrollo de programas y aplicaciones informáticas.

1.2 Determinar los roles y responsabilidades

Identificar y describir los roles y responsabilidades relacionados con el desarrollo de programas y aplicaciones informáticas.

1.3 Desarrollar propuesta de solución

Para cada proyecto informático en lo adelante proyecto, se desarrolla una propuesta inicial de solución técnica que incluye el plan de resultados y el costo del programa y aplicación informática, y tiene en cuenta que:

1. La solución técnica contiene el alcance, los objetivos, los componentes de software del sistema y la tecnología de desarrollo.
2. En la determinación del costo del programa y aplicación informática se tiene en cuenta el resultado de las estimaciones iniciales de parámetros del proyecto tales como: tiempo, esfuerzo y recursos.
3. En los programas y aplicaciones informáticas que se desarrollen a la medida de un cliente, se le entrega la propuesta de solución conciliada.

1.4 Concebir e iniciar el proyecto

Definir formalmente la creación del proyecto y el equipo de trabajo, además de otorgar la autoridad necesaria jefe de emplear los recursos con que cuente o con los que la organización ponga a su disposición. Se pactan con el cliente los documentos y partes del desarrollo del programa y aplicación informática final que le son entregadas.

1.5 Capacitar al personal

Definir y ejecutar un plan de capacitación al personal vinculado al desarrollo de aplicaciones informáticas, con el objetivo de asegurar que posea las habilidades y competencias necesarias para la ejecución del rol que desempeña**.**

1.6 Identificar y socializar el conocimiento

Identificar el conocimiento que se genera y que pueda ser utilizado en el desarrollo de aplicaciones informáticas.

El conocimiento identificado se socializa y permite que se encuentre disponible y pueda ser consultado o analizado, según las necesidades específicas.

El conocimiento puede ser tácito o explícito. Tácito se refiere al conocimiento implícito en las personas y explícito se refiere al conocimiento que ha sido documentado y almacenado en algún tipo de medio.

1.7 Proteger los bienes del cliente

Identificar, controlar y salvaguardar los bienes suministrados por el cliente para utilizarlos en el proyecto o incorporarlos al programa y aplicación informática.

2.- EN LA GESTIÓN DE PROYECTO

2.1 Definir el alcance y objetivos del proyecto

Especificar el alcance y los objetivos que tiene el proyecto, a partir de las necesidades y restricciones del cliente, así como de la propia organización.

El alcance y los objetivos del proyecto se definen inicialmente como parte de la propuesta de solución técnica a través de la regla 1.3.

2.2 Realizar estimaciones

Especificar la estimación pactada con el cliente con el objetivo de desglosar en actividades la planificación inicial y optimizar los recursos asignados o con los que disponga.

La estimación pactada con el cliente es la estimación inicial de los parámetros del proyecto que se obtiene al cumplir la regla 1.3.

2.3 Definir ciclo de vida del proyecto

Definir el ciclo de vida del proyecto donde se establecen las fases e iteraciones por las que transita. El ciclo de vida es coherente con la metodología seleccionada, el alcance, el entorno, los recursos y las restricciones del proyecto.

2.4 Definir un plan de proyecto

Definir el plan de proyecto que incluya un cronograma de ejecución basado en el ciclo de vida, donde se reflejen los principales hitos y actividades del proyecto. También se planifican todas las áreas de impacto en el cumplimiento de los objetivos, tales como gestión de la calidad, gestión de recursos de riesgos, de requisitos, de la configuración y de adquisiciones, monitoreo y pruebas que se consideren necesarias.

2.5 Monitorear y controlar los planes del proyecto

Monitorear y controlar los planes del proyecto a partir de los valores reales de las tareas y lo planificado inicialmente. Se implementan acciones para resolver y prevenir los problemas cuando ocurran desviaciones de los planes que comprometan el cumplimiento de los hitos del proyecto.

2.6 Identificar necesidades de adquisición

Identificar las necesidades que tiene el proyecto de adquirir productos o componentes de software y analizar sus costos y beneficios.

2.7 Seleccionar proveedores y establecer acuerdo y contrato

Identificar los proveedores potenciales de programa y aplicación informática o componentes de software que cubran las necesidades de adquisición del proyecto y establecer un acuerdo y contrato con los seleccionados.

3.- EN LA INGENIERÍA

3.1 Gestionar requisitos

Identificar, especificar e interrelacionar los requisitos del programa y aplicación informática y de sus componentes de software. Los requisitos identificados son aceptados formalmente por el cliente siempre que el desarrollo sea personalizado.

3.2 Desarrollar requisitos

Realizar una descripción técnica de los requisitos y agruparlos acorde con las decisiones arquitectónicas tomadas.

El desarrollo de los requisitos se puede realizar a través de modelos de casos de uso, Modelo del dominio, Escenario de operación, Modelo de proceso de negocio u otros y podrían ser agrupados en módulos o subsistemas.

3.3 Definir la arquitectura del sistema

Definir y aprobar la arquitectura del sistema con los involucrados relevantes, que sirva de base la construcción de la solución y proporcione la información necesaria para su mantenimiento y soporte. La arquitectura contiene:

a. los elementos arquitectónicamente significativos;
b. las definiciones estructurales y la relación entre componentes de software;
c. las principales decisiones arquitectónicas tomadas (patrones, plataforma tecnológica, componentes de software reutilizables);

d. los atributos de calidad a satisfacer con la implementación del programa y aplicación informática.

3.4 Ejecutar pruebas

Ejecutar las pruebas necesarias para verificar los requisitos funcionales y no funcionales del programa y aplicación informática con el apoyo de herramientas manuales o automatizadas que garanticen su objetividad; registrar las no conformidades detectadas y realizar el seguimiento correspondiente.

4. EN EL SOPORTE

4.1 Realizar mediciones a través de indicadores

Establecer indicadores para la gestión del proyecto que permitan satisfacer las necesidades de información a partir de la medición de los objetivos. Analizarlos periódicamente para mantenerlos actualizados.

4.2 Gestionar la Configuración de Software

Identificar los elementos de configuración de software (ECS) y establecer una organización con códigos para cada elemento que permita su mejor identificación y consulta, y disponer un sistema que almacene y controle las versiones. Crear las líneas base y controlar sus cambios, así como las modificaciones de los requisitos de software.

4.3 Realizar el Aseguramiento de la Calidad

Realizar evaluaciones periódicas a la ejecución de los procesos y a sus productos de trabajo, para asegurar la conformidad con los planes, procedimientos y estándares definidos.

Registrar las no conformidades identificadas durante las evaluaciones y asignarle acciones correctivas.

Realizar el seguimiento de las no conformidades hasta la solución definitiva.

ANEXO 2

GLOSARIO DE TÉRMINOS Y DEFINICIONES

1. **Componente de software:** elemento de un sistema de software que ofrece un conjunto de servicios, o funcionalidades, a través de interfaces definidas.
2. **Evaluador autorizado:** persona jurídica autorizada por el Ministerio de Comunicaciones como proveedor de servicio público de evaluación de procesos y de programas y aplicaciones informáticas.
3. **Titular:** persona natural o jurídica propietaria del programa y aplicación informática que es evaluado.
4. **Pruebas de usabilidad:** pruebas realizadas a los programas y aplicaciones informáticas para comprobar la factibilidad del uso.

RESOLUCIÓN No. 166/2017

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero del 2013, en su apartado Primero, numeral Onceno, establece que el Ministerio de Comunicaciones tiene entre sus funciones específicas la de establecer y controlar la aplicación de las normas relativas a la integridad y privacidad de la información que circula por las redes de telecomunicaciones, radiocomunicaciones e informáticas, asegurando su seguridad e invulnerabilidad, el diseño y documentación de los sistemas informáticos, así como la inviolabilidad de los envíos postales.

POR CUANTO: La Resolución Conjunta de los ministros de Finanzas y Precios y de la Informática y las Comunicaciones, de fecha 8 de abril del 2004, puso en vigor los Requisitos para los sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación, y estableció en su apartado Cuarto, la obligatoriedad de que todos estos sistemas cuenten con una Certificación otorgada por la entidad ministerial que se designe al efecto, previo dictamen de una Comisión ad-hoc, integrada por especialistas de ambos Ministerios, sobre la seguridad y protección del sistema y el grado de adaptación a las normas contable cubanas.

POR CUANTO: La Resolución No. 12 del entonces Ministro de la Informática y las Comunicaciones, de fecha 24 de enero del 2005, puso en vigor los requisitos informáticos adicionales para los sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación, la que resulta necesario derogar con la finalidad de lograr una norma jurídica más actualizada.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el inciso a), del Artículo 100 de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el procedimiento para la obtención del certificado del grado de correspondencia de los sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación con los requisitos informáticos que garantizan la seguridad y calidad en su utilización, que como Anexo No. 1 forma parte integrante de la presente Resolución.

SEGUNDO: Las personas que desarrollen o comercialicen sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación que se utilicen por personas jurídicas, cumplen los requisitos a que se refiere el apartado anterior.

TERCERO: A los efectos de la presente Resolución los términos que se relacionan a continuación, tienen el significado siguiente:

a. **Actualización:** adiciones al software que pueden evitar o corregir problemas, aumentar la seguridad del sistema, o bien mejorar el rendimiento de éste.
b. **Cambio de versión:** modificaciones específicas a un producto de software.

c. **Cambio de versión mayor:** modificación de un producto de software que implica agregar nuevas funcionalidades claves, cambios que impacten en la actividad financiero-contable, de impacto para el usuario, como puede ser la inclusión de uno o varios módulos, refleja un cambio visual y funcional notable respecto a la versión anterior.
d. **Cambio de versión de corrección:** modificación de un producto de software que implica corrección de fallos no perceptibles.
e. **Versiones opcionales:** representan modificaciones internas que se le realizan a un producto de software.
f. **Versión no estable:** representa la liberación de una versión de prueba de un producto de software.

CUARTO: Disponer que los sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación que se utilicen por personas jurídicas, cuenten con un certificado otorgado por la Dirección General de Informática, en lo adelante DGI, del Ministerio de Comunicaciones, que asegura el cumplimiento de los requisitos informáticos establecidos. Este proceso no excluye la observancia de la legislación vigente en materia de compatibilización de las inversiones.

QUINTO: Disponer que para autorizar a una entidad a que dictamine el grado de correspondencia de los sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación con los requisitos informáticos que garantizan la seguridad, ésta presenta una solicitud por escrito a la Oficina de Seguridad para las Redes Informáticas, en lo adelante OSRI, del Ministerio de Comunicaciones.

La solicitud se acompaña por un documento acreditativo de su objeto social, o la resolución del jefe de la entidad que faculta para la prestación de este servicio o su misión; una fundamentación de la solicitud que explique las condiciones existentes para realizar esta actividad, así como un aval del nivel técnico profesional de sus especialistas.

La OSRI evalúa la solicitud y dispone de hasta sesenta (60) días para emitir la autorización que permita a la entidad brindar este servicio a terceros, cuando cumplan los requisitos que se detallan en el Anexo No. 2 que forma parte integrante de la presente Resolución.

SEXTO: Las personas que desarrollen o comercialicen sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación, por sí o mediante sus representantes solicitan los dictámenes de seguridad y de calidad a las entidades autorizadas a tales efectos, en caso de calidad corresponde a la DGI la designación de esta.

SÉPTIMO: La autorización y el certificado emitido por la OSRI y la DGI respectivamente, tiene una vigencia de dos (2) años y deben ser renovados en los noventa (90) días antes del vencimiento del plazo, mediante la presentación de la solicitud de renovación a la OSRI o la DGI según corresponda.

OCTAVO: La entidad autorizada a efectuar la evaluación no puede divulgar la información de los sistemas contable–financieros que le es entregada por la persona que desarrolla o comercializa, debe garantizar su confidencialidad y acordar mediante contrato el tratamiento a los productos evaluados, de

forma que no se viole el derecho de autor de estos, según la legislación vigente en dicha materia.

NOVENO: La persona que desarrolla o comercializa entrega para la evaluación, además de las solicitudes de dictámenes, lo siguiente:

1. El programa o aplicación desarrollada y el paquete de instalación;
2. el manual de explotación, que incluya las tablas de relación de la base de datos;
3. el manual de usuario;
4. carta donde se acredita por la máxima autoridad de la persona desarrolladora o comercializadora, a quien se designe para formalizar todo lo referente a dichos trámites; y
5. la información que los evaluadores soliciten al interesado de acuerdo con el tipo de programa o aplicación informática que se evalúa.

DÉCIMO: Las entidades autorizadas a efectuar los dictámenes de evaluación de la seguridad y calidad del sistema, luego de recibir la información suministrada por el solicitante, concilian con estos el tiempo de evaluación y que no puede exceder noventa (90) días para realizarlos. Concluido estos, entregan a la DGI un informe de las pruebas practicadas y de las no conformidades detectadas, y al solicitante los dictámenes correspondientes de calidad y seguridad que avalen o no al sistema para su utilización.

UNDÉCIMO: Las personas que desarrollen o comercialicen por sí o mediante sus representantes los sistemas, presentan los dictámenes de evaluación favorable de seguridad y calidad antes mencionados y el correspondiente al “Grado de adaptación a las normas contable cubanas de los sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación” establecido por la legislación vigente del Ministro de Finanzas y Precios, acompañados de la solicitud correspondiente que se relaciona en el Anexo No. 3, a la DGI, a través de la Dirección Territorial de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico que le corresponda por su domicilio, en lo adelante Dirección Territorial, con el objetivo de que sean valorados por la Comisión Interministerial.

DUODÉCIMO: Una vez emitido el dictamen de la Comisión Interministerial, y de resultar favorable este, la DGI dispone de quince (15) días hábiles para emitir el certificado de aprobación del sistema y entregarlo al interesado a través de la Dirección Territorial correspondiente. El certificado tiene una vigencia de dos (2) años.

Las personas que desarrollen o comercialicen por sí o mediante sus representantes abonan por la emisión o renovación del certificado cincuenta ($50) pesos cubanos (CUP) Este pago se hace directamente en el Banco según se establece por legislación vigente del Ministerio de Finanzas y Precios y la copia del comprobante de pago se presenta a la dirección territorial correspondiente.

La DGI inscribe en el Control Administrativo Central Interno del Ministerio de Comunicaciones los sistemas contable–financieros aprobados por esta y los publica en su sitio Web para conocimiento general.

DÉCIMO TERCERO: La renovación del certificado debe ser solicitada a la DGI a través de la Dirección Territorial que le corresponda con hasta sesenta (60) días de antelación a la fecha de vencimiento del

plazo de vigencia de este, mediante la presentación del documento de solicitud de renovación. El procedimiento es similar al de la solicitud inicial, e incluye en este caso el código del certificado anterior y renovar los dictámenes de seguridad, de calidad y la correspondencia con el "Grado de adaptación a las normas contable cubanas del Sistema Contable–Financiero soportado sobre las Tecnologías de la Información y la Comunicación". Debe presentarse un nuevo documento de acreditación del representante de la entidad, siempre que haya existido cambio al respecto. Una vez transcurrido el plazo de vigencia y sin haberse gestionado la renovación del certificado, los desarrolladores o comercializadores por si o mediante sus representantes, no pueden comercializar el sistema, hasta que obtenga el nuevo certificado para lo que efectúan todos los trámites nuevamente.

DÉCIMO CUARTO: Se requiere de la obtención de un nuevo certificado del sistema, cuando se realice un cambio de versión mayor del sistema contable financiero según lo que se expresa en el anexo No. 4, al considerarse estos como un nuevo sistema. Los cambios de versión menor, de versión de corrección o de versiones opcionales requieren de renovación al vencimiento del plazo de vigencia del certificado expedido.

DÉCIMO QUINTO: Las actualizaciones del sistema que hayan corregido fallos que afecten la experiencia del usuario con el producto o se hayan corregido fallos no perceptibles o poco perceptibles al usuario, requiere su notificación con la información sobre la numeración de la actualización de este a la DGI y vencido el plazo del certificado actual en la renovación se incluye esta.

DÉCIMO SEXTO: Las personas que desarrollen o comercialicen sistemas contable–financieros soportados sobre las Tecnologías de la Información y la Comunicación, por si o mediante sus representantes, quedan obligados a informar a sus clientes sobre las actualizaciones y nuevas versiones para que estos procedan a su actualización.

DÉCIMO SÉPTIMO: La DGI se encarga de evaluar las variaciones de las actualizaciones o cambios de versión de los sistemas para revocar el certificado a los sistemas contable–financieros que no se permiten su utilización por parte de los clientes, tales decisiones se publican en el Sitio Web Público del ministerio, para conocimiento general.

DÉCIMO OCTAVO: La personas que implanten sistemas contable–financieros a partir de la fecha de entrada en vigor de la presente resolución dejan constancia por escrito de las condiciones de seguridad con que queda desplegado el sistema.

DÉCIMO NOVENO: El cliente debe reportar toda vulnerabilidad detectada en los sistemas contable–financieros aprobados y en explotación, a la persona que desarrolla para su corrección y a la DGI, quien informa a las entidades correspondientes. Los desarrolladores deben habilitar la vía y forma para el reporte.

VIGÉSIMO: Los incidentes de violación de seguridad detectados en la explotación de los sistemas contable–financieros se reportan al CuCert de la Oficina de Seguridad para las Redes informáticas perteneciente a este ministerio por los mecanismos habilitados para ello en su sitio web.

VIGÉSIMO PRIMERO: La Dirección General de Informática, la Dirección de Inspección, la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y las oficinas territoriales de control del Ministerio de Comunicaciones, quedan encargadas del control del cumplimiento de lo que por la presente se dispone.

VIGÉSIMO SEGUNDO: Todo incumplimiento de lo que se establece por la presente, detectado por las oficinas territoriales de control, las Direcciones Territoriales de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y por la Oficina de Seguridad para las Redes Informáticas se le notifica a la persona desarrolladora o comercializadora, además se envía copia de la notificación a la dirección de la instancia a la que esta se subordina, y al Director General de Informática de este Ministerio, quien en dependencia del tipo de incumplimiento detectado envía copia al Director de Política Contable del Ministerio de Finanzas y Precios, a la Contraloría General de la República o al Ministerio del Interior, según corresponda.

VIGÉSIMO TERCERO: La Comisión Interministerial evalúa el incumplimiento detectado y en dependencia de su impacto o la reincidencia de este, dictamina la invalidación del certificado emitido por la DGI. La invalidación no exime de la responsabilidad civil, administrativa o penal que se derive de este hecho.

VIGÉSIMO CUARTO: A la entrada en vigor de la presente resolución aquellos sistemas que hayan recibido de la DGI el certificado de aprobación del sistema, mantienen su vigencia hasta su vencimiento y para renovarlo aplican lo que por la presente se establece. En caso de no obtener el certificado el desarrollador o comercializador puede volver a solicitar este una vez solucionadas las vulnerabilidades detectadas.

VIGÉSIMO QUINTO: Encargar al Director de la DGI la elaboración de la actualización de los requisitos informáticos que garantizan la seguridad y calidad de los sistemas contable financieros y proponer al Director de Regulaciones la actualización del marco jurídico que corresponda.

VIGÉSIMO SEXTO: La DGI queda responsabilizada con la elaboración de los procedimientos necesarios para la implementación de lo dispuesto en la presente en un plazo de treinta (30) días a partir de su publicación en la Gaceta Oficial de la República de Cuba.

VIGÉSIMO SÉPTIMO: Derogar la Resolución No. 12 del Ministro de la Informática y las Comunicaciones, de fecha 24 de enero del 2005.

VIGÉSIMO OCTAVO: La presente Resolución entra en vigor a los treinta (30) días posteriores de la fecha de su publicación en la Gaceta Oficial de la República de Cuba.

DISPOSICIÓN TRANSITORIA

ÚNICA: Las funciones establecidas en la presente a la Dirección General de Informática relativas a la emisión y renovación del certificado de aprobación de los sistemas contable–financieros, se transfieren por el que suscribe a la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, una vez esta culmine su proceso de perfeccionamiento funcional, estructural y composicional.

DÉSE CUENTA a la Ministra de Finanzas y Precios, al Ministro del Interior y a la Contralora General de la República.

NOTIFÍQUESE a los directores generales de Informática y de la Oficina de Seguridad para las Redes Informáticas, así como a los directores de Regulaciones y de Inspección, pertenecientes al Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, pertenecientes todos al Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 16 días del mes de mayo de 2017.

Maimir Mesa Ramos
Ministro

Anexo No. 1 Resolución No. 166/2017

REQUISITOS INFORMÁTICOS DE SEGURIDAD Y CALIDAD PARA LOS SISTEMAS CONTABLE-FINANCIEROS SOPORTADOS SOBRE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

A.- REQUISITOS INFORMÁTICOS DE SEGURIDAD

1. Implementar sistemas y base de datos de forma segura, que incluye la activación de las trazas que estos tienen implementadas y además cumplan con los requisitos de protección informática de la información, la técnica y las comunicaciones establecidos en las normativas vigentes sobre seguridad para las tecnologías de la información y la comunicación;

2. proteger la información primaria que se gestiona en los sistemas contable-financieros, como mínimo mediante los mecanismos siguientes:

a. Control de acceso; y
b. cifrado de datos.

3. generar alertas ante intentos de violación de la seguridad o alteración de la información del sistema y permitir trazabilidad de las operaciones ejecutadas y manipulaciones en la Base de Datos;

4. permitir el trabajo en red y ser multiusuarios;

5. permitir que cada usuario gestione sus propias credenciales de acceso una vez que esté dentro del sistema y que estas cumplan con la legislación vigente sobre seguridad informática;

6. considerar en el diseño, desde el punto de vista de usabilidad, la sencillez de empleo del sistema mediante una información clara, navegación intuitiva y seguridad, así como otras facilidades con ese objetivo;

7. contar con la posibilidad de ser modificado y/o actualizado a versiones superiores, con la correspondiente documentación y los ficheros contentivos de los códigos fuentes;

8. posibilitar la interoperabilidad entre los diferentes módulos del sistema, los cuales deben tener personalizados los accesos;

9. implementar mecanismos de seguridad orientados a impedir la exportación de datos susceptibles de ser modificados, sin emplear las funcionalidades del sistema; y

10. definir un administrador del Sistema Contable -financiero para la tramitación de los permisos y roles.

B.- REQUISITOS INFORMÁTICOS DE CALIDAD

Se evalúan los requisitos informáticos de calidad de acuerdo con las Normas Cubanas vigentes sobre Ingeniería de Software y sistemas – Requisitos de Calidad y Evaluación de Software (SQuaRE) – Modelos de la Calidad de Software y Sistemas y sobre Tecnologías de la Información y la Comunicación – Paquete de Software – Requisitos de calidad y pruebas, donde se comprueban características de Calidad, tales como: usabilidad, adecuación funcional, eficiencia de desempeño, fiabilidad, portabilidad y seguridad.

Anexo No. 2 Resolución No. 166/2017

REQUISITOS A CUMPLIR POR LAS ENTIDADES FACULTADAS PARA EMITIR EL DICTAMEN DE SEGURIDAD DE LA CORRESPONDENCIA DE LOS SISTEMAS CONTABLES FINANCIEROS SOPORTADOS SOBRE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Los requisitos a tener en cuenta a tales efectos son los siguientes:

a) Nivel técnico de los especialistas que laboren en la entidad;

b) que el objeto social, o facultad para la prestación de este servicio o la misión de dicha entidad coincida con estos fines;

c) que dicha entidad cuente con mecanismos eficientes que garanticen la calidad y respuesta rápida de los servicios;

d) que la entidad esté realmente en condiciones de cumplir los reglamentos y disposiciones establecidos en esta materia;

e) que las herramientas tecnológicas de protección y seguridad técnica de los sistemas informáticos que utilicen estén debidamente certificados por las instituciones correspondientes; y

f) que el capital sea enteramente nacional y el personal designado para brindar los servicios esté integrado por ciudadanos cubanos que residan de forma permanente en el país.

Anexo No. 3 Resolución No. 166 /2017

MODELO DE SOLICITUD DE CERTIFICACIÓN DE SISTEMA CONTABLE-FINANCIERO SOPORTADO SOBRE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Solicitud de certificación de sistemas contable-financieros soportados sobre las TIC	
Fecha de solicitud:	Acrónimo del sistema:
Datos del sistema a certificar	
Versión:	Motor de la base de datos:
Nombre completo:	
Nacionalidad:	

Datos de la persona o entidad solicitante		
Acrónimo:		
Nombre completo:		
Teléfono:	Correo electrónico:	
Dirección:		
Organismo o institución al que pertenece o con el cual se relaciona en el país:		
Datos del representante de la persona o entidad para los trámites de certificación:		
Cargo en la entidad:	Número de carnet de identidad o pasaporte:	
Teléfono:	Correo electrónico:	Firma:
Dictámenes presentados		
Dictamen sobre cumplimiento de los requisitos informáticos de seguridad, emitido por:		
Dictamen sobre cumplimiento de los requisitos informáticos de calidad, emitido por:		
Dictamen sobre cumplimiento del grado de adaptación a las normas contable cubanas emitido por:		

Anexo No. 4 Resolución No. 166 /2017

DESCRIPCIÓN DEL CAMBIO DE VERSIÓN Y ACTUALIZACIÓN DE UN PRODUCTO DE SOFTWARE

El versionado de todo producto de software debe definirse en cuatro (4) niveles, de ellos tres (3) requeridos relacionados con los cambios de versión mayor, menor y de corrección, uno (1) opcional relacionado con versiones opcionales y se puede incluir como quinto nivel las versiones no estables, y quedan identificados de la forma siguiente:

a.b.c. [v] _ alpha|beta|RC

Donde:
a = indica la versión mayor, que durante el desarrollo inicial debe ser igual a cero (0), y no se incrementará hasta que no se haya liberado una primera versión del producto.
b = indica la versión menor.
c = indica la versión de corrección.
v = versiones opcionales.
alpha|beta|RC =indican la versión no estable.
a,b,c y v son números enteros y positivos.

Criterios para el cambio de versión.
El cambio de versión se hará incrementalmente, por lo que a, b y c se incrementarán en uno (1) ante el cambio de la versión correspondiente.

a) Los incrementos en la versión mayor tienen lugar cuando:

1. Se han agregado nuevas funcionalidades claves, de impacto para el usuario, como puede ser la inclusión de uno o varios módulos.
2. La nueva versión del producto refleja cambio visual y funcional notable respecto a la versión anterior.
3. Se realiza cambio del gestor de Base de Datos.

b) Los incrementos en la versión menor tienen lugar cuando:

1. Se han hecho cambios significativos en la forma en la que se ofrecen las funcionalidades ya existentes.
2. Se han corregido fallos que afectaban la experiencia del usuario con el producto.
3. Las funcionalidades ofrecidas por el producto han evolucionado de forma perceptible para el usuario.

c) Los incrementos en la versión de corrección tienen lugar cuando:

1. Se han corregido fallos no perceptibles, o poco perceptibles al usuario.
2. Se han hecho mejoras al producto no perceptibles, o poco perceptibles al usuario.

d) **Las versiones opcionales** contienen tanta numeración como la persona desarrolladora considere necesario para cambios internos al producto, acorde a la representación en el versionado.

e) **las versiones no estables** representan una liberación específica que tiene en cuenta el momento del ciclo de vida en el que se encuentra el producto de software y el propósito de cada liberación. Solo se agrega al versionado cuando se desea liberar una versión para probar el producto, en cualquier otro caso debe ser obviada y contendrá solo uno de sus valores siguientes:

1. La versión alpha es aquella liberación del producto que se hace para el uso interno de la persona desarrolladora. Aunque posee poca estabilidad puede servir para mostrar algunas funcionalidades y hacer pruebas internas.
2. La versión beta es la liberación que tiene un grado aceptable de estabilidad y que se usa externamente a la persona desarrolladora para su sometimiento a pruebas. Incluso puede ser mostrada a los usuarios para obtener sus criterios sobre el producto antes de lanzar la versión definitiva.
3. La versión RC (Release Candidate) es la liberación que tiene un alto grado de estabilidad y es candidata a la versión final del producto.

Por ejemplo:

1. al haber cambio de versión menor en 1.9.0, la nueva versión es 1.10.0
2. al haber cambio de versión mayor en 0.2.6, la nueva versión es 1.0.0
3. al haber cambio de versión de corrección en 1.1.1.1.1.1, la nueva versión es 1.1.1.2.0.0_alpha

Actualizaciones de software tienen como objetivo reparar problemas específicos de vulnerabilidades que se presentan en un programa, frecuentemente se liberan a través de parches que los desarrolladores o comercializadores de software publican en sus sitios WEB para que los usuarios las descarguen.

RESOLUCIÓN No. 165/2012

POR CUANTO: El Acuerdo No. 3736 del Comité Ejecutivo del Consejo de Ministros, de fecha 18 de julio del 2000, en su numeral Séptimo, Apartado Segundo, dispone que el Ministerio de la Informática y las Comunicaciones es el organismo encargado de establecer, regular y controlar las normas técnicas y operacionales de todas las redes informáticas y sistemas de comunicaciones en general, nacionales e internacionales que funcionan en el país.

POR CUANTO: La Resolución Ministerial No. 145 del 20 de junio de 2008, del Ministro de Informática y las Comunicaciones establece los Indicadores de Calidad de los Servicios de Datos, con sus valores asociados que tienen que ser garantizados por los proveedores de servicios públicos de acceso a Internet, los que resultan necesario actualizar adecuándolos al desarrollo de los nuevos

servicios que estos proveedores prestan a los usuarios finales.

POR TANTO: En el ejercicio de la facultad conferida por el numeral Cuarto Apartado Tercero del Acuerdo No. 2817 del Comité Ejecutivo del Consejo de Ministros, de fecha 25 de noviembre de 1994;

RESUELVO:

PRIMERO: Aprobar los Indicadores de Calidad, sus métricas y valores asociados de los Servicios de Datos, en lo adelante Indicadores de Calidad, que se detallan en los Anexos No. 1; 2; 3 y 4 que forman parte integrante de esta Resolución.

SEGUNDO: A los efectos de la presente Resolución, se adoptan los términos y definiciones siguientes:

Calidad de servicio percibida. Nivel de la calidad de servicio en que se especifican los parámetros de cada servicio que el usuario percibe y puede comprobar y que determinan su mayor o menor satisfacción con el servicio percibido, por ejemplo: éxito de la conexión y disponibilidad del servicio, calidad del audio o el video o la velocidad de transferencia de ficheros.

Prestaciones funcionales de red. Nivel de la calidad de servicio que se corresponde con especificaciones técnicas de red cuyo cumplimiento implica que la calidad de servicio percibida es la adecuada. Incluye los parámetros técnicos de red de primer nivel, por ejemplo, pérdidas de paquetes o retardo de extremo a extremo, que son comprobados, reportados en un formato comparable y publicados por los proveedores de forma que sean entendibles por los usuarios (los parámetros técnicos de red de segundo nivel son gestionados internamente por los proveedores a nivel de soporte del transporte y encaminamiento).

Prestaciones no funcionales de red. Nivel de la calidad de servicio que incluye los parámetros que definen los aspectos de provisión, gestión y mantenimiento del servicio que básicamente reflejan el nivel de gestión que el usuario percibe en su relación con el proveedor, como por ejemplo, tiempo de demora en atención a las quejas o precisión y corrección en la facturación. Métricas. Definición de parámetros, métodos de medición y muestreo y métodos de agregación de medidas. En particular, para cada uno de los niveles especificados anteriormente, definen, para cada uno de ellos, los valores, umbrales y procedimientos de medición.

Clase de calidad de servicio. Clasificación de la calidad del servicio de red que tiene por objetivo establecer las bases de los acuerdos entre los usuarios finales y los proveedores de servicio de red, y entre los proveedores de servicio. Se clasifican desde la clase 0 hasta la 5, aunque esta última no se especifica.

TERCERO: La información complementaria que, como mínimo, suministra el proveedor en sus contratos a sus usuarios sobre la facturación, uso y tráfico de los enlaces contratados de los servicios brindados de transmisión de datos se encuentra en el Anexo No. 4 formando parte integrante

de la presente Resolución.

CUARTO: La presente actualización de los Indicadores de Calidad debe ser implementada en los contratos y los servicios que presta el proveedor, como máximo, dentro de los ciento ochenta (180) días posteriores a su publicación en la Gaceta Oficial de la República de Cuba, tomando en cuenta para ello los valores expuestos, considerados como norma u otros valores que impliquen una mayor calidad en los servicios prestados.

QUINTO: El proveedor informará anualmente a la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, los valores estadísticos promedio de los indicadores establecidos por la presente, antes de finalizar el mes de marzo, correspondiendo el cierre de la información al 31 de diciembre de cada año.

SEXTO: Los proveedores presentan a la Dirección de Regulaciones y Normas del ministerio, en el plazo referido en el apartado Cuarto, los procedimientos para la medición de los valores asignados en la presente actualización de los Indicadores de Calidad, a los fines de su conciliación.

SÉPTIMO: La Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, es la encargada de receptar, organizar y preservar la información relacionada con los valores estadísticos anuales de los Indicadores de Calidad establecidos por los apartados Tercero y Cuarto, emitiendo un informe analítico a la Dirección del Ministerio de la Informática y Comunicaciones, con los resultados de estas y otras acciones de control y supervisión.

OCTAVO: Encargar a la Dirección de Regulaciones y Normas de este Ministerio para que realice las propuestas de modificación sobre la actualización de los Indicadores de Calidad que se establecen por la presente Resolución, tomando en cuenta el desarrollo de los nuevos servicios que sean ofertados.

NOVENO: Derogar la Resolución Ministerial No. 145 de fecha 20 de junio de 2008 y cualquier norma de igual o inferior jerarquía que se oponga a lo que por la presente se dispone.

NOTIFÍQUESE al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba S.A., ETECSA, a la Directora de la Empresa Tecnologías de la Información y Servicios Telemáticos, CITMATEL, perteneciente al Ministerio de Ciencias, Tecnología y Medio Ambiente, al Director General de la Agencia de Control y Supervisión y al Director de la Dirección de Regulaciones y Normas, ambos del Ministerio de la Informática y las Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los días 16 del mes de octubre de 2012.

Maimir Mesa Ramos
Ministro

ANEXO No. 1

INDICADORES DE CALIDAD SERVICIOS DE DATOS. PRESTACIONES NO FUNCIONALES

Los Indicadores de Calidad prestados por los proveedores de Servicios Públicos de Acceso a Internet, relacionados con las prestaciones no funcionales, se exponen a continuación en la tabla No. 1.

Tabla No. 1. Prestaciones no funcionales.

No.	Métricas		
	Indicador de calidad	**Valor**	**UM**
1.1	**Plazos para el inicio o activación de la provisión de los servicios**		
1.1 a)	**Servicios Dedicados**	30	días
1.1 b)	**Servicios Conmutados**		
	• Sin configuración en el usuario	Inmediato	
	• Con configuración en el usuario	7	días
1.1 c)	**Servicios de Hospedaje de Sitios**	7	días
1.2	**Plazo de resolución de incidencias de los servicios dedicados** (tiempo de reparación)	60	horas
1.3	**Número de reclamaciones de por cada 1,000 usuarios**	20	-

INFORMACION ADICIONAL

1.1 Plazos para el inicio o activación de la provisión de los servicios.

a) Para Servicios Dedicados:
Una vez recibida la solicitud por escrito del usuario, el proveedor dispondrá del tiempo establecido en la tabla No. 1 para proveer el servicio dedicado, previa confirmación de la aceptación por este último al solicitante.

b) Servicios Conmutados:
Después de recibida la solicitud y confirmada esta, el proveedor proveerá el servicio en el plazo establecido en la tabla No. 1. Para el caso que el servicio tenga que ser configurado en el sitio, ello

se refiere al domicilio del usuario.

c) Servicios de Hospedaje de Sitios:

Recibida la solicitud y confirmada la misma, el proveedor proveerá el servicio en el plazo establecido en la tabla No. 1, con posterioridad a la entrega de la información (disco compacto) por parte del usuario.

En cada uno de los tres servicios anteriores, si la solicitud es denegada por dificultades técnico-económicas, lo cual se notifica al solicitante, el proveedor la toma en cuenta como demanda insatisfecha y trabaja para crear las condiciones técnicas necesarias, con el objetivo de ofrecer este tipo de servicio. Una vez que estas condiciones sean creadas se le confirma la aceptación de la solicitud al usuario.

En el caso de que el proveedor no proporcionara los servicios antes relacionados, dentro de la fecha prevista de puesta a disposición de los mismos y no pudiera demostrar que la causa del retraso no le es imputable, el usuario tiene derecho a exigir una compensación por retraso en la entrega, tal y como se detalla en la tabla siguiente:

Tabla No. 1.1 Compensación como descuento de la cuota de Instalación.

Retraso (en días laborables)	Descuento de la cuota mensual (%)
De 1 a 5	5
De 6 a 10	10
Más de 1 1	20

1.2 Plazo de resolución de incidencias de los servicios dedicados:

El tiempo máximo de reparación de las averías que afectan los servicios dedicados del usuario (véase la tabla No. 2) no incluye los tiempos de inactividad planificados por el proveedor, debidos al mantenimiento programado, informado con antelación por el operador. En caso de incumplimiento de lo expuesto, en la tabla No. 2, se realizarán descuentos en la cuota mensual según la siguiente tabla:

Tabla No. 1.2 Compensación como descuento de la cuota mensual de servicio afectado.

Tiempo de reparación por encima de lo que debe garantizar el proveedor (horas)	Descuento de la cuota mensual (%)
De 0.5 a 1	2.5
De 1 a 1.5	5
Más de 1.5 y hasta 72	7
Mas de 72	La compensación será de acuerdo a la cantidad de días sin servicio.

ANEXO No. 2

INDICADORES DE CALIDAD SERVICIOS DE DATOS. CALIDAD DE SERVICIO PERCIBIDA

Los Indicadores de Calidad prestados por los proveedores de Servicios Públicos de Acceso a Internet, relacionados con la calidad de servicio percibida, se exponen a continuación en la tabla No. 2.

Tabla No. 2. Calidad de servicio percibida.

No.	Métricas		
	Indicador de calidad	Valor	UM
2.1	Disponibilidad del Servicio de Alojamiento (Coubicado) de Servidores	99.5	%
2.2	Disponibilidad del Servicio Dedicado	95	%
2.3	Disponibilidad de los Servidores y Servicios	99.5	%
2.4	Anchura de Banda	100	%

PRECISIONES

La garantía de la calidad percibida de los servicios de datos que oferta el proveedor se asegura por tipo de servicio:

2.1 Disponibilidad del Servicio de Alojamiento de Servidores:

La garantía de disponibilidad del servicio de alojamiento de servidores tiene en cuenta la provisión entre otros de la alimentación eléctrica, climatización, seguridad lógica y física, red e iluminación (véase la tabla No. 2). En caso de incumplimiento se realizarán descuentos en la cuota mensual según la siguiente tabla No. 2.1.

Tabla No. 2.1. Compensación del tiempo de indisponibilidad, como descuento de la cuota mensual del servicio afectado.

Indisponibilidad del servicio en el mes (h)	Descuento de la cuota mensual (%)
De 3 a 5	2.5
De 5 a 7	5
Más de 7 y hasta 72	7
Más de 72	Será de acuerdo a la cantidad de días sin servicio.

Esta garantía no cubre las interrupciones siguientes:
(a) Circuitos o equipos propiedad del usuario, o en el caso en que, siendo aquellos propiedad de ETECSA, se haya plasmado contractualmente su gestión y seguridad por parte del usuario.
(b) Fallos en el hardware del equipo del usuario.
(c) Actos negligentes o indebidos del usuario.
(d) Causas de fuerza mayor.
(e) Otras causas que sin constituir fuerza mayor no son imputables al proveedor.

2.2. Disponibilidad del Servicio Dedicado:

El proveedor debe garantizar la disponibilidad mensual de los servicios de datos e Internet (véase la tabla No. 2). En caso de incumplimiento se realizarán descuentos en la cuota mensual según la siguiente tabla No. 2.2:

Tabla No. 2.2. Compensación del tiempo de indisponibilidad, como descuento de la cuota mensual del servicio afectado.

Indisponibilidad del servicio (horas)	Descuento de la cuota mensual (%)
De 3 a 5	2.5%
De 5 a 7	5%
Más de 7 y hasta 72	7%
Mas de 72	Será de acuerdo a la cantidad de días sin servicio.

Esta garantía no cubre las interrupciones siguientes:
(a) Circuitos o equipos propiedad del usuario, o en el caso en que, siendo aquellos propiedad de ETECSA, se haya plasmado contractualmente su gestión y seguridad por parte del usuario.
(b) Fallos en el hardware del equipo del usuario.
(c) Actos indebidos u omisiones del usuario.
(d) Causas de fuerza mayor.
(e) Otras causas que sin constituir fuerza mayor no son imputables al proveedor.

2.3. Disponibilidad de los Servidores y Servicios:

El proveedor debe garantizar la disponibilidad de sus servidores y servicios (véase la tabla No. 2) lo que incluye la garantía de funcionamiento de los elementos, tanto de hardware como de software, (servidores DNS, E-mail, bases de datos, copias de seguridad u otros que correspondan), que componen el servicio. Los mantenimientos programados no se incluyen en los cálculos de disponibilidad. En caso de incumplimiento se realizarán descuentos en la cuota mensual según la siguiente tabla No. 2.3:

Tabla No. 2.3 Compensación del tiempo de indisponibilidad, como descuento de la cuota mensual del servicio afectado.

Indisponibilidad del servicio (h)	Descuento de la cuota mensual (%)
De 3 a 5	5
De 5 a 7	7
Mayor de 7	30

Esta garantía no cubre las interrupciones siguientes:

(a) Circuitos o equipos propiedad del usuario, o en el caso en que, siendo aquellos propiedad de ETECSA, se haya plasmado contractualmente su gestión y seguridad por parte del usuario.

(b) Fallos en el hardware del equipo del usuario,

(c) Actos indebidos u omisiones del usuario.

(d) Causas de fuerza mayor.

(e) Otras causas que sin constituir fuerza mayor no son imputables al proveedor.

2.4. Anchura de Banda:

El proveedor debe garantizar la anchura de banda (de acuerdo con los valores de la tabla No. 2) contratada por el usuario para los servicios de Internet hasta el NAP (Punto de Acceso a la Red). Su incumplimiento y comprobación por el usuario puede dar lugar a una reclamación cuyo reporte deberá de efectuarse en el momento de ocurrencia de la incidencia y de comprobarse por los especialistas del proveedor, ello dará lugar a una indemnización del 5% de la cuota mensual del servicio.

ANEXO No. 3

INDICADORES DE CALIDAD SERVICIOS DE DATOS. PRESTACIONES FUNCIONALES DE RED

Los Indicadores de Calidad prestados por los proveedores de Servicios Públicos de Acceso a Internet, relacionados con las prestaciones funcionales de red por tipo de servicio se exponen a continuación en la tabla No. 3.

Tabla No. 3. Prestaciones funcionales de red por tipo de servicio.

No.	Métricas		
	Indicador de calidad	Valor	UM
3.1	Clase de servicios 0 (video conferencia IP; videotelefonía; difusión de video o por demanda, de alta definición)		
3.1.1	Retardo de transferencia de paquetes IP (IPTD)	100	ms
3.1.2	Variación del IPTD (IPDV)	50	ms
3.1.3	Tasa de pérdidas de paquetes IP (IPLR)	$1x10^{-3}$	
3.1.4	Tasa de errores de paquetes IP (IPER)	$1x10^{-4}$	
3.2	Clase de servicios 1(Voz IP, ADSL, GPRS)		
3.2.1	Retardo de transferencia de paquetes IP (IPTD)	400	ms
3.2.2	Variación del IPTD (IPDV)	50	ms
3.2.3	Tasa de pérdidas de paquetes IP (IPLR)	$1x10^{-3}$	
3.2.4	Tasa de errores de paquetes IP (IPER)	$1x10^{-4}$	
3.3	Clase de servicios 2 (señalización, juegos)		
3.3.1	Retardo de transferencia de paquetes IP (IPTD)	100	ms
3.3.2	Tasa de pérdidas de paquetes IP (IPLR)	$1x10^{-3}$	
3.3.3	Tasa de errores de paquetes IP (IPER)	$1x10^{-4}$	
3.4	Clase de servicios 3 (datos transaccionales interactivos, navegación, ciber-charla)		
3.4.1	Retardo de transferencia de paquetes IP (IPTD)	400	ms
3.4.2	Tasa de pérdidas de paquetes IP (IPLR)	$1x10^{-3}$	
3.4.3	Tasa de errores de paquetes IP (IPER)	$1x10^{-4}$	

No.	Métricas		
	Indicador de calidad	Valor	UM
3.5	Clase de servicios 4 (transacciones cortas, datos en grandes cantidades, correo, P2P)		
3.5.1	Retardo de transferencia de paquetes IP (IPTD)	1	s
3.5.2	Tasa de pérdidas de paquetes IP (IPLR)	$1x10^{-3}$	
3.5.3	Tasa de errores de paquetes IP (IPER)	$1x10^{-4}$	

PRECISIONES

Las prestaciones funcionales de red de datos que oferta el proveedor se asegura por el tipo de servicio en correspondencia con la clase en que clasifique. En caso de incumplimiento se realizarán descuentos en la cuota mensual según la siguiente tabla No. 3.1:

Tabla No. 3.1 Compensación como descuento de la cuota mensual del servicio por afectación del indicador.

Clase de servicios			
Tipo de servicio	Índice	AFECTACIÓN	COMPENSACIÓN
0 video conferencia IP; videotelefonía; difusión de video o por demanda, de alta definición	IPTD, IPDV IPLR IPER	Incumplimiento de cualquiera de los indicadores durante el mes	Descuento de tres días en los gastos mensuales del servicio
1 Voz IP, ADSL, GPRS	IPTD, IPDV IPLR IPER	Idem	Idem
2 señalización, juegos	IPTD, IPDV IPLR IPER	Idem	Idem
3 datos transaccionales interactivos, navegación, ciber - charla	IPTD IPLR IPER	Idem	Idem
4 transacciones cortas, datos en grandes cantidades, correo, P2P	IPTD IPLR IPER	Idem	Idem

Por reporte reiterado se entiende la apertura de más de tres reportes por la misma causa dentro del mes.

Los mantenimientos programados no se incluyen en los cálculos de disponibilidad.

Los incumplimientos y su comprobación por el usuario pueden permitir una reclamación cuyo reporte deberá de efectuarse en el momento de ocurrencia de la incidencia y de comprobarse por los especialistas del proveedor, dará lugar a la indemnización prevista en la tabla No. 2.1. Esta garantía no cubre las afectaciones provocadas por las siguientes causas:

(a) Circuitos o equipos propiedad del cliente.
(b) Fallos en el hardware o software del equipo del cliente.
(c) Actos negligentes o indebidos del cliente.
(d) Causas de fuerza mayor.
(e) Otras causas que sin constituir fuerza mayor no son imputables al proveedor.

ANEXO No. 4

INDICADORES DE CALIDAD SERVICIOS DE DATOS. INFORMACIÓN A SUMINISTRAR AL USUARIO

El proveedor implementa un sistema que brinda una información a sus usuarios sobre la facturación, el uso y/o tráfico de los servicios contratados de transmisión de datos.

A continuación se desglosa la información según el tipo de servicio contratado.

Facturación: Tanto para los enlaces conmutados como para los enlaces digitales dedicados, el usuario tiene siempre la opción de poder chequear su facturación, accediendo directamente a la facturación del mes en curso, la cual estará disponible como máximo siete (7) días hábiles después de comenzado el mes en la página de los datos de facturación del proveedor. Además de acceder al histórico de sus facturaciones anteriores, desde el mes anterior y hasta seis (6) meses atrás. Los nuevos usuarios deben tener información de facturación disponible a partir del mes siguiente al inicio de su servicio.

a) Enlaces conmutados:

El usuario conoce y verifica en línea el estado actual de utilización del servicio contratado y en virtud de ello realiza un uso racional de sus recursos. También debe poder detectar si su cuenta está siendo utilizada por otras personas sin su debida autorización. Puede también verificar cuál fue su contabilidad en el mes anterior.

b) Enlaces digitales dedicados:

El usuario tiene acceso a estadísticas de mediciones de tráfico, diaria (promedio de 5 minutos), semanal (promedio de 30 minutos), mensual (promedio de 2 horas) y anual (promedio de un día).

Estos servicios tanto en el caso de los enlaces conmutados, como en el de los enlaces digitales dedicados, deben ser brindados por el proveedor de forma gratuita para el usuario y consultados por

los mismos en línea.

c) Puertos conmutados sobre la Plataforma Pública de Acceso Conmutado (PAP): A solicitud del usuario, éste puede recibir la siguiente información:

1. Cantidad de puertos utilizados (Diario, Semanal y Mensual).
2. Fecha y hora en que los usuarios establecen la conexión.
3. Intentos fallidos de conexión por indisponibilidad de puertos.

d) Hospedaje virtual: El usuario dispone de la siguiente información estadística en línea (Día/ Mes/Año):

1. Índice de Accesos (número de accesos/cantidad de usuarios).
2. Números IP con mayor acceso.
3. Accesos por meses.
4. Hora con mayor actividad del sitio.
5. Días de la semana con mayor acceso.
6. Módulos con mayor acceso.

RESOLUCIÓN No. 85/2007

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000 cambió la denominación del Ministerio de Comunicaciones por el de Ministerio ce la Informática y las Comunicaciones, para que desarrollara las tareas y funciones que realizaba el Ministerio de Comunicaciones así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria ‘Sideromecánica y la Electrónica

POR CUANTO: El Consejo de Estado de la República de Cuba mediante Acuerdo de fecha 30 de Agosto del 2006, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: El Acuerdo No. 2817 de fecha 28 de noviembre de 1994, del Comité Ejecutivo del Consejo de Ministros, faculta a los Jefes de los Organismos de la Administración Central del Estado; a dictar en el límite de sus facultades y competencia reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del organismo y sus dependencias

POR CUANTO: El Acuerdo No. 3736. de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo del Consejo de Ministros, establece que el Ministerio de la Informática y las Comunicaciones, en lo adelante MIC, es el organismo encargado de proponer la estrategia, orientar y controlar la elaboración de Programas de Acción para la aplicación acelerada de la informática y las comunicaciones en los órganos del Estado y del Gobierno en todos los niveles, evaluar los aspectos tecnológicos y económicos relacionados con este proceso y hacer las propuestas que correspondan con este objetivo. Establecer, regular y controlar la política para la fabricación, homologación y

certificación de equipos, partes, accesorios y sistemas en su esfera de competencia para uso nacional, así como las regulaciones técnicas relacionadas con la importación de los mismos.

POR CUANTO: Es necesario atemperar el uso y explotación eficiente de los sistemas informáticos de que dispone el país tanto por personas jurídicas como naturales al proceso de ahorro energético que se desarrolla nacionalmente.

POR TANTO: En el ejercicio de las facultades que me están conferidas,

RESUELVO:

PRIMERO: Aprobar las medidas que deberán tenerse en cuenta para el ahorro de energía en los sistemas informáticos existentes en el país y que se relacionan en el resuelvo tercero.

SEGUNDO: A los efectos de la presente resolución, los términos que se citan a continuación tienen el siguiente significado;

1. **Ahorro de energía:** La cantidad de energía ahorrada, determinada mediante la medición y/o estimación del consumo antes y después de la aplicación de una o más medidas de mejora de la eficiencia energética, al tiempo que se tiene en cuenta la normalización de las condiciones externas que influyen en el consumo de energía.

2. **Computador:** Toda unidad de mesa, torre o minitorre, o portátil, los ordenadores personales, las estaciones de trabajo, los terminales de redes. Estos aparatos deberán poder abastecerse de corriente a partir de la red, pero esto no excluirá a las unidades que lo hacen a partir de la red y también de una batería. Esta definición se refiere esencialmente a los ordenadores para utilizarse en empresas o los hogares, no incluye los servidores.

3. **Monitor:** Todo dispositivo de visualización de tubo catódico, o pantalla de panel plano (por ejemplo, un indicador de cristal líquido), o cualquier otro dispositivo de visualización. incluidos sus componentes electrónicos asociados, que puede venderse por separado o integrado en el chasis del ordenador. Esta definición se refiere esencialmente a los monitores estándar destinados a utilizarse con los ordenadores.

4. **Sistema informático:** Sistema que se compone de un ordenador y un monitor y puede ser integrado en un solo chasis o no.

5. **Inactividad:** El período de tiempo durante el cual un ordenador no recibe ninguna entrada del usuario (por ejemplo, pulsación de teclado o movimiento de ratón).

6. **Modo de bajo consumo o de «espera»:** El estado de consumo reducido al que pasa el ordenador tras un período de inactividad.

7. **Sucesos de activación:** Todo suceso o estímulo provocado por el usuario, programado o exterior

que provoca en el ordenador la transición de su modo de bajo consumo/«espera.» a su modo activo de funcionamiento. Los ejemplos de sucesos de activación incluyen, sin limitarse a ellos, el movimiento del ratón, la pulsación del teclado o el accionamiento de botón en los chasis, y en el caso de sucesos exteriores, los estímulos provocados por vía telefónica, por control remoto a partir de la red, del MODEM. etc.

8. **Modo Desactivado (Stand by):** Modo de consumo de energía mínimo que puede mantenerse por tiempo indefinido cuando el ordenador o monitor están conectados a la red eléctrica. Es el estado de consumo en que el ordenador o monitor están conectados a una fuente de electricidad, esta preparado para pasar al modo activo de funcionamiento mediante un suceso de activación.

9. **Modo Desactivado completo:** Modo cuando el ordenador y monitor están desconectados de la red eléctrica. Pueden existir dos modalidades de este modo:
a. El equipo ha sido desenchufado de la red completamente.
b. El equipo está enchufado a la red pero se desconecta, por medio de un interruptor de desactivación completa (regleta, regulador de voltaje, fuente de respaldo (UPS) u otro).

10. **Hibernación:** Este modo ajusta la CPU y los periféricos al modo de menor consumo de energía posible, todo lo que está en memoria es guardado en el disco duro. Cuando se reinicia el equipo este queda exactamente como cuando se apagó.

TERCERO: Las medidas que deberán tenerse en cuenta para el ahorro de energía de los sistemas informáticos existentes en el país se relacionan a continuación:

1. Activar el Modo de bajo consumo o de «espera»:

1.1. Configurar la opción de ahorro para el monitor La pantalla se apagará después del tiempo seleccionado de inactividad, volviendo a encenderse al tener lugar un suceso de activación como por ejemplo con sólo mover el ratón (mouse).
1.2. Configurar la opción de ahorro para el disco duro. Esta opción contribuye al ahorro pues el disco duro se mantiene en permanente actividad aunque no se use la computadora.
1.3. Configurar la opción de ahorro inactividad del PC; esta actúa al igual que el punto 1.1 pero para el PC

Para configurar el ahorro en el monitor, PC y en el disco duro se deberá hacer lo siguiente: ir a Inicio. Configuración, Panel de Control. Pantalla, Protector de Pantalla, botón Energía y en las Combinaciones de Energía seleccionar e lapso de tiempo para pasar al modo de bajo consumo o de espera del disco, el monitor y el PC. Se recomienda entre cinco y diez minutos para el monitor y para el disco duro y entre 15 y 30 minutos para la opción inactividad del PC.

2. Habilitar el modo de hibernación.

Habilitar este modo en aquellas computadoras que lo poseen. Se recomienda seleccionar como lapso de tiempo para pasar al modo de hibernación un tiempo no menor de dos horas y no mayor de 6 horas.

3. Desconectar los equipos por la noche.
Los equipos en estado desactivado permanecen consumiendo energía por lo que se recomienda desconectar el sistema informático por la noche (al concluir la jornada de trabajo). Esta desconexión debe realizarse según los modos explicados en el Resuelvo segundo, punto 9.

4. Instalación de un software para el ahorro de energía.
Como alternativa a las medidas de ahorro energético debe aplicarse la instalación en el computador de un software que permita el apagado del mismo. Cada organismo debe implementar la instalación de este software y la política a seguir, fundamentalmente en el horario pico (6PM a 10 PM).

CUARTO: Los Organismos de la Administración Central del Estado (OACE) e Instituciones Nacionales deberán garantizar el cumplimiento de lo dispuesto en la presente Resolución, instrumentando las medidas de divulgación, control y supervisión internas que sean necesarias para logar el objetivo propuesto.

QUINTO: La Dirección de Comunicación Institucional del MIC deberá coordinar con los medios, la divulgación masiva por estas vías de las acciones aprobadas por la presente resolución.

SEXTO: Encargar a la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, la instrumentación de las medidas de control y supervisión pertinentes para garantizar el cumplimiento de lo dispuesto en la presente Resolución y a la Dirección de Regulaciones y Normas, de implementar la emisión de normativas complementarias que sean necesarias para su mejor cumplimiento.

COMUNIQÚESE a los Viceministros, a las Direcciones de Regulaciones y Normas, Comunicación Institucional, a la Agencia de Control y Supervisión, a la Oficina de Seguridad de Redes Informáticas, a la Oficina para la Informatización así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLIQUESE en la Gaceta Oficial de la República de Cuba.

Dada en la ciudad de La Habana, a los 18 días del mes de Mayo del 2007.

Ramiro Valdés Menéndez
Ministro

RESOLUCIÓN CONJUNTA /2004 MFP – MIC

POR CUANTO: El Acuerdo No. 2817 del Comité Ejecutivo del Consejo de Ministros de fecha 25 de Noviembre de 1994, en su apartado tercero, inciso 4, autoriza a los Ministros de Finanzas y Precios y de Informática y las Comunicaciones a dictar, en el límite de sus facultades y competencias, Reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del Organismo y en su caso, para los demás Organismos, los órganos locales del Poder Popular, las entidades estatales, el sector cooperativo, mixto, privado y la población.

POR CUANTO: El Acuerdo No. 3736 del Comité Ejecutivo del Consejo de Ministros, de fecha 18 de julio del 2000, faculta al Ministerio de la Informática y las Comunicaciones, para establecer y controlar las normas y regulaciones relativas a la integridad de la información, la seguridad e invulnerabilidad de las redes de infocomunicaciones; el diseño y la documentación de los sistemas informáticos.

POR CUANTO: El Acuerdo No. 3944 del Comité Ejecutivo del Consejo de Ministros, de fecha 19 de marzo del 2001, faculta al Ministerio de Finanzas y Precios, elaborar y en su caso, proponer la legislación y los sistemas que aseguren la integridad y el control financiero de los intereses del Estado cubano en entidades públicas, privadas y asociaciones con capital extranjero, incluyendo los principios, normas y procedimientos de contabilidad, costos y control interno.

POR CUANTO: La Resolución Conjunta del Comité Estatal de Finanzas, actualmente, Ministerio de Finanzas y Precios, en lo adelante MFP y el Instituto Nacional de Sistemas Automatizados y Técnicas de Computación, actualmente extinto y cuyas funciones asume el Ministerio de la Informática y las Comunicaciones, en lo adelante MIC, de fecha 1ro. de agosto de 1991, puso en vigor los requisitos mínimos que deberán cumplir los sistemas automatizados para garantizar el Control Interno y la Auditoría.

POR CUANTO: El Acuerdo No. 092 del Consejo de Ministros, de fecha 2 de junio del 2002, aprobó las Medidas Complementarias para dar continuidad a los esfuerzos dirigidos al fortalecimiento de la Contabilidad y el Control Interno en las entidades y dentro de ellas considera instrumentar la certificación de los sistemas contables – financieros soportados sobre las tecnologías de la información y las comunicaciones.

POR CUANTO: Se hace necesario actualizar los requisitos que deberán cumplir los sistemas contables – financieros soportados sobre las tecnologías de la información y establecer el proceso de certificación de estos sistemas.

POR TANTO: En el ejercicio de las facultades que nos están conferidas,

RESOLVEMOS:

PRIMERO: Poner en vigor los "Requisitos para los Sistemas Contables – Financieros soportados sobre las tecnologías de la información", que como anexo, forma parte integrante de esta Resolución.

SEGUNDO: Los requisitos a que se refiere el apartado anterior serán de obligatorio cumplimiento para todas las personas naturales y jurídicas que diseñen, elaboren o exploten, sistemas y programas contables – financieros soportados sobre tecnologías de la información.

TERCERO: Las personas jurídicas que explotan sistemas y programas contables – financieros sustentados en las tecnologías de la información están obligadas a imprimir al cierre del ejercicio económico anual, los registros contables con independencia del sistema que esté en explotación y a conservar los listados y la información en soporte electrónico según la legislación vigente.

CUARTO: Se establece la obligatoriedad de que todos los sistemas contables – financieros soportados sobre las tecnologías de la información, cuenten con una CERTIFICACIÓN otorgada por la entidad ministerial que se designe al efecto, previo dictamen de una comisión "ad-hoc" integrada por Especialistas de ambos Ministerios, sobre:

- Seguridad y protección del sistema.
- Grado de adaptación a las normas contables cubanas.

QUINTO: En los casos en que se considere necesario, podrán participar en la comisión especialistas de otros organismos de la administración central del Estado.

SEXTO: La Agencia de Control y Supervisión del MIC habilitará un Registro de Control de las certificaciones expedidas.

SÉPTIMO: A todos los efectos de este proceso, el Ministerio de la Informática y las Comunicaciones y el Ministerio de Finanzas y Precios, dictarán los procedimientos que se requieran.

OCTAVO: Los productores o representantes de Sistemas Contables – Financieros soportados sobre las tecnologías de la información que estén en explotación al momento de la promulgación de esta resolución, tendrán un plazo máximo de un año para certificar el sistema, informar a sus clientes del resultado y continuar su comercialización si se certifica el sistema.

NOVENO: Los jefes de las entidades, en el momento de seleccionar un sistema, deberán exigir a los productores o representantes de Sistemas Contables – Financieros soportados sobre las tecnologías de la información, la documentación que acredita que el sistema está certificado por la autoridad competente.

DÉCIMO: Se delega en los viceministros que atienden a la Dirección de Normas Contables del

Ministerio de Finanzas y Precios y el que atiende la Oficina Nacional de Seguridad para las Redes Informáticas del Ministerio de la Informática y las Comunicaciones, la facultad para dictar cuantas instrucciones resulten necesarias para el mejor cumplimiento de la presente.

UNDÉCIMO: Se deroga la Resolución Conjunta CEF – INSAC, de fecha 1ro. de agosto de 1991 y cuantas más normas y disposiciones se opongan a lo dispuesto.

COMUNIQUESE la presente Resolución a cuantas personas naturales y jurídicas deben conocer de la misma.

PUBLÍQUESE en la Gaceta Oficial de la República y archívense los originales en las Direcciones Jurídicas de ambos Ministerios.

DADA en la ciudad de La Habana, a los ocho días del mes de abril del 2004.

Georgina Barreiro Fajardo	**Ignacio González Plana**
Ministra	**Ministro**
Ministerio de Finanzas y Precios	**Ministerio de la Informática y las Comunicaciones**

ANEXO
REQUISITOS PARA LOS SISTEMAS CONTABLES FINANCIEROS SOPORTADOS SOBRE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Introducción

La utilización de los sistemas contables financieros soportados sobre las tecnologías de la información está sujeta al cumplimiento de las exigencias vigentes en materia de seguridad informática para estas tecnologías, no obstante, a partir de la importancia que para cualquier organización representa este tipo de sistemas y de sus particularidades, resulta conveniente especificar los principales requerimientos que en los mismos deben ser considerados.

Sobre esta base, el presente documento expresa los requisitos que deben tenerse en cuenta durante el ciclo de vida de los sistemas contables financieros soportados sobre las tecnologías de la información y las comunicaciones.

Responsabilidades

Los usuarios de las tecnologías de la información para la Explotación de un Sistema Contable Financiero en una entidad tienen las siguientes obligaciones principales:

a) Adquirir la preparación necesaria y los conocimientos de Seguridad Informática imprescindibles

para el desempeño de su trabajo.

b) Contar con la autorización expresa del jefe facultado, para obtener acceso a cualquier activo o recurso.
c) No divulgar la información a que tiene acceso sin la autorización del Jefe facultado.
d) Cumplir los procedimientos establecidos para el empleo de las contraseñas y para la salva de programas y datos.
e) No introducir ni utilizar en las tecnologías ningún producto ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.
f) No intentar transgredir ninguna de las medidas de seguridad establecidas.
g) Proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada, dañada o usada la información que contiene o utilizado el sistema al que esté conectada.
h) Informar al dirigente facultado de cualquier anomalía de seguridad detectada.

Identificación, Autenticación y Control de Acceso

El acceso de los usuarios a los sistemas contables financieros de una entidad tiene que estar aprobado previamente por la dirección de la misma y constar evidencia documental de ese acto.

El equipamiento utilizado en los sistemas contables financieros no podrá ser utilizado por personal que no esté debidamente autorizado.

En cada entidad se definirán los procedimientos que se requieran para otorgar o suspender el acceso de los usuarios a los sistemas contables financieros y los perfiles de trabajo de los mismos. Estos procedimientos incluirán la conformación de un listado de usuarios autorizados con sus derechos de acceso, garantizando la eliminación de aquellos que ya no los requieran por razones de trabajo o por no laborar en la entidad, así como de los identificadores, junto a todos los derechos de acceso que le fueron concedidos.

A las tecnologías de información utilizadas para la explotación de los sistemas contables financieros se les implementarán mecanismos para identificar y autenticar a los usuarios, así como para garantizar el registro y conservación de todos los accesos e intentos fallidos de acceso.

Para la protección de los sistemas y la protección del propio usuario, las contraseñas:

- Tienen que ser privadas e intransferibles.
- Su estructura y fortaleza estará en correspondencia con el acceso que protegen.
- No pueden ser visualizadas en pantalla mientras se teclean.
- No pueden ser almacenadas en texto claro (sin cifrar) en ningún tipo de tecnologías de información.
- Se guardará copia de las mismas, de forma que se garantice su privacidad, para su empleo como excepción en caso de ausencia del usuario.

De la integridad de los sistemas, ficheros y datos.

Se implementarán los mecanismos de seguridad que eviten la modificación, destrucción y pérdida de los ficheros y datos vinculados con los sistemas contables financieros.

Se establecerán, por las entidades, las medidas para proteger los programas del sistema y sus procedimientos de control para evitar que puedan ser violados, borrados o modificados con el fin de evadir los controles de seguridad.

Los programas, ficheros y datos de los sistemas contables financieros, incluyendo las copias de respaldo no pueden ser, en ningún caso:

- Accedidos públicamente sin la debida autorización.
- Los accesos temporales tienen que estar plenamente justificados y aprobados, así como ser eliminados inmediatamente después de terminar la necesidad de su uso.
- Las actividades de uso y acceso realizadas por los usuarios, tienen que ser registradas y revisadas.

Se garantizará la existencia de pistas o rastros de seguimiento que posibiliten las investigaciones más comunes que se realizan sobre las operaciones, tales como las cuentas que fueron afectadas por una transacción, la emisión de una factura, las retenciones que afectaron el salario devengado, y otras similares.

Del trabajo en sistemas multiusuarios

En las tecnologías de información que brindan servicio a varios usuarios, como sistemas multiusuarios, servidores de bases de datos, aplicaciones con más de un operador y otros casos similares, se implementarán mecanismos de control que permitan contar con una traza o registro de los principales eventos que se ejecuten, por lo que:

- En los sistemas de redes se controlará el acceso al servidor o a las terminales.
- Estará debidamente compartimentado y controlado el acceso a los ficheros o bases de datos de los sistemas de forma tal que se garantice la identificación de dicho acceso.

De los procedimientos de salva de los ficheros de datos y el sistema

En cada entidad se establecerán los procedimientos que garanticen:

- La obtención de copias de seguridad actualizadas de programas y datos.
- La frecuencia con que se realicen.
- Los responsables de la ejecución de los procedimientos.
- La cantidad de copias, según su importancia.

- Que cada salva esté adecuadamente identificada.
- Se mantengan copias de seguridad para datos y programas en algún soporte magnético externo.
- Las copias de seguridad se conserven en locales alejados de donde se procesa habitualmente.

6. COMERCIALIZACIÓN E IMPORTACIÓN

RESOLUCIÓN No. 110/2020

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros, de 22 de mayo de 2017, en su numeral Octavo, apartado Primero, establece que el Ministerio de Comunicaciones tiene la función específica de regular y controlar las especificaciones técnicas y de explotación de los sistemas, equipos y dispositivos a emplear en las redes de telecomunicaciones e informáticas, para garantizar la interconexión entre las redes públicas, así como la interoperabilidad de los servicios.

POR CUANTO: Resulta necesario modificar la relación de equipos y dispositivos de telecomunicaciones/TIC según las partidas arancelarias reguladas en la Resolución 132 de 25 de junio de 2019 del Ministro de Comunicaciones, que requieren o no de Autorización Técnica expedida por Ministerio de Comunicaciones para la importación.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Autorizar los equipos y dispositivos relacionados en el Anexo Único que forma parte de la presente Resolución, los que no requieren de la correspondiente Autorización Técnica del Ministerio de Comunicaciones para su importación.

SEGUNDO: Corresponde al Director General de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones elaborar el procedimiento y las medidas de control y supervisión para garantizar el cumplimiento de lo dispuesto en la presente Resolución.

DESE CUENTA al Jefe de la Aduana General de la República.

NOTIFÍQUESE al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A, a los Presidentes del Grupo Empresarial de la Informática y las Comunicaciones y al de Correos de Cuba; a los directores generales de Comunicaciones, de Informática y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico ya los directores de las oficinas territoriales de control, del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Defensa y de la Oficina de Seguridad para las Redes Informáticas y a los directores de Regulaciones y de Inspección, todos del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

DADA en la Habana, a los 26 días del mes de octubre del 2020.

Jorge Luis Perdomo Di-Lella

ANEXO UNICO RESOLUCIÓN

NOMENCLATURA DE PRODUCTOS DE IMPORTACION SEGÚN SACLAP VIGENTE QUE NO REQUIEREN AUTORIZACION TÉCNICA DEL MINISTERIO DE COMUNICACIONES

PARTIDAS y SUBPARTIDAS	DESCRIPCIÓN
De la partida 8443	Máquinas y aparatos para imprimir mediante planchas, cilindros y demás elementos impresores de la partida 84.42; las demás máquinas impresoras, copiadoras y de fax, incluso combinadas entre sí; partes y accesorios:
Se libera la subpartida	
	- Las demás maquinas impresoras, copiadoras y de fax, incluso combinadas entre sí:
8443.3100	-- Máquinas que efectúan dos o más de las siguientes funciones: impresión, copia o fax, aptas para ser conectadas a una máquina automática para tratamiento o procesamiento de datos o a una red.
8443.3200	-- Las demás, aptas para ser conectadas a una máquina automática para tratamiento o procesamiento de datos o a una red.
8443.3900	-- Las demás.
De la partida 8471	Máquinas automáticas para tratamiento o procesamiento de datos y sus unidades; lectores magnéticos u ópticos, máquinas para registro de datos sobre soporte en forma codificada y máquinas para tratamiento o procesamiento de estos datos, no expresados ni comprendidos en otra parte.
Se liberan las subpartidas	

8471.3000	- Máquinas automáticas para tratamiento o procesamiento de datos, portátiles, de peso inferior o igual a 10 kg, que estén constituidas al menos, por una unidad central de proceso, un teclado y un visualizador.
	- Las demás máquinas automáticas para tratamiento o procesamiento de datos:
8471.4100	-- Que incluyan en la misma envoltura, al menos, una unidad central de proceso y, aunque estén combinadas, una unidad de entrada y una de salida.
8471.4900	-- Las demás presentadas en forma de sistemas.
8471.5000	- Unidades de proceso, excepto las de las subpartidas 8471.41 u 8471.49, aunque incluyan en la misma envoltura uno o dos de los tipos siguientes de unidades: unidad de memoria, unidad de entrada y unidad de salida.
8471.6000	- Unidades de entrada o salida, aunque incluyan unidades de memoria en la misma envoltura.
8471.7000	- Unidades de memoria.
8471.8000	- Las demás unidades de máquinas automáticas para tratamiento o procesamiento de datos.
8471.9000	- Los demás.
De la partida 8473	Partes y accesorios (excepto los estuches, fundas y similares) identificables como destinados, exclusiva o principalmente, a las máquinas o aparatos de las partidas 84.70 a 84.72.
Se liberan las subpartidas	
8473.3000	-Partes y accesorios de máquinas de la partida 84.71.
8473.5000	-Partes y accesorios que puedan utilizarse indistintamente con máquinas o aparatos de varias de las partidas 84.70 a 84.72.
De la partida 8504	Transformadores eléctricos, convertidores eléctricos estáticos (por ejemplo: rectificadores) y bobinas de reactancia (autoinducción).
Se libera la subpartida	
8504.4000	- Convertidores estáticos
De la partida 8528	Monitores y proyectores, que no incorporen aparato receptor de televisión; aparatos receptores de televisión, incluso con aparato receptor de radiodifusión o grabación o reproducción de sonido o imagen incorporado.
Se liberan las subpartidas	
	- Monitores con tubo de rayos catódicos:
8528.4200	- Aptos para ser conectados directamente y diseñados para ser utilizados con máquinas automáticas para tratamiento o procesamiento de datos de la partida 84.71.
	- Los demás monitores:

8528.5200	- Aptos para ser conectados directamente y diseñados para ser utilizados con máquinas automáticas para tratamiento o procesamiento de datos de la partida 84.71.
	- Proyectores:
8528.6200	- Aptos para ser conectados directamente y diseñados para ser utilizados con máquinas automáticas para tratamiento o procesamiento de datos de la partida 84.71.

RESOLUCIÓN No. 132/2019

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros, de 22 de mayo de 2017, en su numeral Octavo, apartado Primero, establece que el Ministerio de Comunicaciones tiene la función específica de regular y controlar las especificaciones técnicas y de explotación de los sistemas, equipos y dispositivos a emplear en las redes de telecomunicaciones e informáticas, para garantizar la interconexión entre las redes públicas, así como la interoperabilidad de los servicios.

POR CUANTO: Resulta necesario actualizar la relación de equipos y dispositivos de telecomunicaciones y de Tecnologías de la Información y la Comunicación así como establecer el Reglamento sobre evaluación de la conformidad y homologación de equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación que emite el Ministerio de Comunicaciones, con el fin de que los equipos que se importen, fabriquen o se comercialicen en el país, garanticen el buen funcionamiento de las redes públicas de telecomunicaciones y de Tecnologías de la Información y la Comunicación y la seguridad de los usuarios, el empleo racional y eficiente del espectro radioeléctrico y evitar la ocurrencia de interferencias a otros servicios de telecomunicaciones, por lo cual procede emitir una disposición normativa que ordene los aspectos antes referidos.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: La importación de equipos y dispositivos relacionados en el Anexo I y II que forma parte de la presente Resolución, requieren de la correspondiente Autorización Técnica del Ministerio de Comunicaciones, la que debe ser presentada ante la autoridad aduanal a los fines de la importación.

SEGUNDO: Los equipos y dispositivos que se importen de manera temporal y que se ponen en funcionamiento en el territorio nacional, requieren autorización técnica temporal emitida por la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones, en lo adelante UPTCER y se exoneran del cumplimiento de lo que por la presente Resolución se establece.

TERCERO: El importador, de acuerdo al tipo de equipo o dispositivo que pretende importar, sea definitivo o temporal según las descripciones de los anexos y de los documentos que debe presentar, tiene que hacer la solicitud de la Autorización Técnica a la UPTCER con treinta días como mínimo de antelación al arribo al país de estos, de forma que permita hacer los trámites necesarios.

CUARTO: La importación de las muestras de productos que sea sometida a pruebas, se rige por lo establecido en el apartado anterior y el importador debe adjuntar la información técnica cuando realiza la solicitud.

QUINTO: En la importación de los productos que obtuvieron el certificado de homologación o de evaluación de conformidad satisfactoria, se adjunta a la solicitud, el número de código de estos emitidos según el Reglamento aprobado mediante la presente Resolución.

SEXTO: La UPTCER tiene diez días hábiles después de recibida la información relacionada en el apartado anterior, para emitir la Autorización Técnica.

SÉPTIMO: En caso de que el equipo o dispositivo llegue al país y el importador no presente a la autoridad aduanal la Autorización Técnica correspondiente, se procede a la aplicación de lo establecido en las normativas aduaneras.

OCTAVO: Los importadores de las mercancías relacionadas en los anexos I y II de la presente Resolución, que se determinen por la Dirección General de Comunicaciones del Ministerio de Comunicaciones, que no requieran del Certificado de Homologación, ni del documento de evaluación de la conformidad, solicitan la Autorización Técnica a la UPTCER y deben consignar los datos siguientes:

a) nombre del equipo que se importa;
b) marca y modelo de este;
c) partida y subpartida arancelaria;
d) características técnicas principales;
e) fabricante;
f) uso al que se destina.

NOVENO: Los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación que se pretendan importar cuando contengan Sistemas de Protección Criptográfica, debe someterse a la evaluación y aprobación según la legislación vigente del Ministerio del Interior.

DÉCIMO: Los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación autorizados a entrar al país para fines de uso personal o de demostración, los equipos de embarcaciones de recreo y los de radioaficionados construidos por el propio usuario y que no pretendan comercializarse, no se someten al proceso de evaluación de la conformidad ni obtienen el Certificado de Homologación, siempre que no estén sujetos a otras disposiciones específicas.

UNDÉCIMO: Los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación importados por personas jurídicas con carácter comercial que se conecten a las redes públicas de telecomunicaciones y de Tecnologías de la Información y la Comunicación o haga uso del espectro radioeléctrico, tienen que ser sometidos al proceso de evaluación de la conformidad y poseer un Certificado de Homologación expedido por la Dirección General de Comunicaciones.

DUODÉCIMO: Los equipos referidos en el apartado anterior cuando son importados sin carácter comercial de acuerdo a la legislación vigente, según sus disposiciones específicas deben tener una autorización para su uso, que es emitida por la Dirección General de Comunicaciones, y cuando esta considere, puede someterlos al proceso de evaluación de la conformidad y a la obtención de un Certificado de Homologación de ser necesario.

DÉCIMO TERCERO: Aprobar el siguiente*:*

REGLAMENTO SOBRE EVALUACION DE LA CONFORMIDAD Y HOMOLOGACIÓN DE EQUIPOS DE TELECOMUNICACIONES/TIC

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. El objeto del presente Reglamento es el de establecer el conjunto de acciones y operaciones a realizar los importadores, fabricantes y comercializadores para la obtención del Certificado de Homologación de los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación que se conecten a las redes públicas de telecomunicaciones o que hagan uso del espectro radioeléctrico, así como para la obtención del documento de evaluación de la conformidad con las especificaciones técnicas establecidas de los equipos que no requieran homologación.

Artículo 2. Los términos que se citan a continuación tienen el significado siguiente:

a) **Autorización Técnica:** documento emitido por el Ministerio de Comunicaciones para autorizar la importación de equipos destinado a las telecomunicaciones y de Tecnologías de la Información y la Comunicación que cumplen con las legislaciones vigentes y que permite que estos no sean retenidos en frontera por la autoridad aduanal.

b) **Aval técnico:** documento emitido por el Comité de Computadoras o por la Dirección General de Comunicaciones**,** que corresponda con tipo de equipo según el anexo al que pertenezca y que expresa la conformidad de sus características técnicas, y estar acorde con el desarrollo y actualización de la tecnología.

c) **Certificado de Homologación:** documento emitido para una marca y modelo de un equipo destinado a las telecomunicaciones y de Tecnologías de la Información y la Comunicación**,** donde se expresa la aceptación de sus características técnicas y de funcionamiento en su conexión con las redes públicas de telecomunicaciones y de Tecnologías de la Información y la Comunicación o del uso del espectro radioeléctrico, sin producir daños o interferencias perjudiciales a terceros.

d) **Compatibilidad electromagnética:** capacidad de cualquier equipo o aparato de telecomunicaciones y de Tecnologías de la Información y la Comunicación para funcionar de forma satisfactoria en su entorno electromagnético sin provocar perturbaciones de este tipo, de forma tal que pueda operar adecuadamente sin ser interferido y sin causar interferencia a otros equipos, ni interrumpir de alguna forma el funcionamiento normal de estos en ese entorno.

e) **Donativo:** recursos de diversa naturaleza, recibidos con carácter no reembolsable, que contribuyan al desarrollo del país y al enfrentamiento de emergencias por desastres naturales o a cubrir necesidades de la población. Se materializan a través de Donativos Puntuales o Proyectos de Colaboración.

f) **Donativos Puntuales:** recursos recibidos, no asociados a Proyectos de Colaboración.

g) **Equipo de telecomunicaciones y de Tecnologías de la Información y la Comunicación:** dispositivo o conjunto de dispositivos destinados a transmitir o recibir o ambas inclusive, información en forma de signos, señales, escritos, imágenes y sonidos de cualquier naturaleza por medios físicos, electromagnéticos, ópticos, radioeléctricos u otros, y pueden confluir en él más de una función de manera simultánea. También comprende a los módulos que forman parte de un equipo de telecomunicaciones y de Tecnologías de la Información y la Comunicación que hagan posible la conexión a una red o sistema.

h) **Evaluación de la conformidad:** proceso de comprobación del cumplimiento de un equipo y aparato de telecomunicaciones y de Tecnologías de la Información y la Comunicación con las especificaciones técnicas establecidas.

i) **Interoperabilidad:** condición que permite que sistemas o productos de telecomunicaciones y de Tecnologías de la Información y la Comunicación diferentes puedan relacionarse entre sí, sin ambigüedad, para coordinar procesos o intercambiar datos.

j) **Proyectos de Colaboración:** conjunto de acciones articuladas, encaminadas a la realización de uno o varios objetivos, en un período de tiempo determinado, en correspondencia con las prioridades del desarrollo económico y social del país en las esferas de: salud, educación, agropecuaria, ciencia y técnica, medioambiente, cultura, deportes, y otras definidas por el Gobierno de la República de Cuba.

k) **Red pública de telecomunicaciones/TIC:** red de telecomunicaciones y de Tecnologías de la Información y la Comunicación que se explota principalmente para la prestación de servicios públicos de telecomunicaciones y de Tecnologías de la Información y la Comunicación.

CAPÍTULO II

DE LA EVALUACIÓN DE LA CONFORMIDAD Y EL CERTIFICADO DE HOMOLOGACIÓN

Artículo 3. El documento de la evaluación de la conformidad o el Certificado de Homologación constituyen requisitos indispensables para la obtención de la autorización técnica que permita la importación, comercialización y utilización de los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación, aplicable a los de producción nacional y a las donaciones. Este proceso no excluye el cumplimiento de la legislación vigente para la compatibilización de las inversiones.

Artículo 4. La comercialización de determinados tipos de equipos, dispositivos y aparatos en el país requiere, cuando se considere necesario, garantías de servicios de postventa como requisito indispensable para obtener la autorización técnica, para mantener su explotación en el país.

Artículo 5. El resultado del proceso de evaluación de la conformidad de los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación que no requieran homologación, asegura la compatibilidad de las características técnicas de los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación y la seguridad de las tecnologías.

Artículo 6. Para la obtención del Certificado de Homologación se requiere comprobar que los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación cumplan, además de lo señalado en el Artículo precedente, con lo siguiente:

a) Las normas, requisitos de interoperabilidad y la seguridad establecidos para ser conectados a una red pública de telecomunicaciones y de Tecnologías de la Información y la Comunicación;

b) las regulaciones y características técnicas correspondientes al uso del espectro radioeléctrico y verificar la compatibilidad electromagnética.

Artículo 7. El Certificado de Homologación no constituye autorización para la prestación de servicios de telecomunicaciones y de Tecnologías de la Información y la Comunicación.

Artículo 8. La Dirección General de Comunicaciones solicita a los operadores de redes públicas de telecomunicaciones la definición de las características técnicas y de seguridad de sus interfaces disponibles para la conexión.

Artículo 9. La evaluación del cumplimiento de las normas y requisitos de interoperabilidad de los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación en el proceso de obtención del Certificado de Homologación, la realiza la entidad designada por la Dirección General de Comunicaciones o esta última decide en caso de no poder efectuarse la evaluación.

Artículo 10. Los Certificados de Homologación emitidos deben contener:

a) Un código único para cada marca y modelo de equipo de telecomunicaciones/TIC, establecido por la instancia que emite el certificado;

b) fecha de emisión y vencimiento del Certificado;

c) datos técnicos del equipo: descripción, función, marca, modelo, fabricante, ensamblado, partida y subpartida arancelaria y la norma técnica aplicada;

d) resumen de las especificaciones técnicas de funcionamiento, de ser necesario se adiciona una nota con indicación de particularidades.

Artículo 11. Corresponde a la Dirección General de Comunicaciones confeccionar y publicar en el sitio Web del MINCOM, la relación actualizada de los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación, que han obtenido el Certificado de Homologación o el documento de

evaluación de la conformidad satisfactoria porque no requieren ser certificados, con los datos básicos mencionados en el artículo precedente.

CAPÍTULO III

DE LA SOLICITUD DE EVALUACIÓN DE LA CONFORMIDAD Y EL CERTIFICADO DE HOMOLOGACIÓN Y SU RENOVACIÓN

Sección Primera

De la Solicitud de Evaluación de la Conformidad y el Certificado de Homologación

Artículo 12. La evaluación de la conformidad, así como el Certificado de Homologación se solicitan por las personas jurídicas autorizadas a importar, producir, comercializar o entidades extranjeras interesadas, así como por personas naturales y jurídicas para el uso privado de equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación, con excepción de lo expresado en los apartados OCTAVO, DÉCIMO y DÉCIMO SEGUNDO de esta Resolución.

Artículo 13. El interesado presenta a través de la Dirección Territorial de la UPTCER, en lo adelante Dirección Territorial, a la Dirección General de Comunicaciones la solicitud de evaluación de la conformidad o la del Certificado de Homologación, y entregan los datos requeridos mediante aplicación informática en red o modelo aprobado para ello que se encuentra publicado en el sitio Web de Ministerio de Comunicaciones; la Dirección General de Comunicaciones, por estas mismas vías, informa al solicitante en dependencia del tipo de equipo sobre las entidades designadas para hacer las pruebas de evaluación de la conformidad o el Certificado de Homologación.

Artículo 14. El Comité de Computadoras es un órgano colegiado, técnico-asesor para la compra e importación de productos específicos de interés nacional y las partidas y subpartidas controladas por este se encuentran en el Anexo II, el aval técnico emitido por el Comité, constituye el documento de la evaluación de la conformidad satisfactoria de esos equipos, que se utiliza para emitir la Autorización Técnica para la importación.

Artículo 15. Las entidades importadoras que requieran equipos especiales, relacionados con las partidas y subpartidas del Anexo II, que no se encuentran incluidas en su nomenclador autorizado, solicitan el aval técnico del Comité de Computadoras para que sean presentados al Ministerio de Comercio Exterior e Inversión Extranjera, para la aprobación de una importación eventual.

Artículo 16. Las entidades que tengan autorización del Ministerio de Comunicaciones para el uso de equipos de permanencia temporal y deseen dejar definitivamente dichos equipos, requieren autorización de la Dirección General de Comunicaciones para realizar el proceso de obtener el Certificado de Homologación o el documento de la evaluación de la conformidad.

Artículo 17. Las entidades encargadas de tramitar los donativos puntuales o los proyectos de colaboración con financiamiento en el exterior cumplen lo establecido en la presente Resolución, según el anexo al que pertenece dicho equipamiento; en caso de donativos puntuales se solicita el aval técnico

del Comité de Computadoras o de la Dirección General de Comunicaciones de acuerdo al tipo de equipo según los anexos, para que sea presentado al Ministerio de Comercio Exterior e Inversión Extranjera, para la aprobación de su importación.

Artículo 18. Los datos básicos a entregar por el solicitante de evaluación de la conformidad o del Certificado de Homologación son:

a) nombre y descripción del equipo;
b) marca y modelo de este;
c) programa o aplicación informática empleada y su versión;
d) partida y subpartida arancelaria;
e) denominación comercial;
f) fabricante y proveedor;
g) datos técnicos del equipo; y
h) lugar de ensamblaje.

Artículo 19. La modificación de los datos básicos, cambia la descripción del producto por lo que puede ser necesario un nuevo Certificado de Homologación o una nueva evaluación de la conformidad.

Artículo 20. La importación de productos que han obtenido el Certificado de Homologación o el de evaluación de la conformidad satisfactoria con anterioridad y se encuentren publicados en el sitio Web de Ministerio de Comunicaciones, solo necesitan la solicitud de la Autorización Técnica para su importación, que se presenta a la Dirección Territorial a través de la aplicación informática, la que tiene diez días hábiles para emitirla; los equipos procedentes de donativos relativos a las partidas y subpartidas del Anexo II deben obtener además previamente el aval técnico del Comité de Computadoras.

Artículo 21. Los resultados de las pruebas realizadas por la entidad designada son enviados a la Dirección General de Comunicaciones, que dispone de un máximo de treinta días para la entrega al interesado del Certificado de Homologación a través de la Dirección Territorial, o en caso de no ser otorgado, ofrecer por escrito la respuesta y su fundamentación.

Artículo 22. El solicitante tiene la responsabilidad de pagar el precio que se estipule por la realización de las pruebas a la entidad designada, así como abonar cincuenta pesos en la moneda que corresponda por el certificado emitido y por su renovación; este último pago lo realiza el solicitante directamente en la sucursal bancaria o por transferencia bancaria según se establece por legislación vigente del Ministerio de Finanzas y Precios y presenta el comprobante de pago a la Dirección Territorial para la obtención del certificado y la copia se anexa al expediente.

Sección Segunda

De las Pruebas a los Equipos y la entidad designada para esta actividad

Artículo 23. La Dirección General de Comunicaciones y Dirección General de Informática, según corresponda por el tipo de equipamiento, son las encargadas de determinar las entidades que realizan

las pruebas a estos en el ámbito específico de las telecomunicaciones y de Tecnologías de la Información y la Comunicación, así como también la de aceptar o no, los certificados emitidos por los laboratorios extranjeros reconocidos internacionalmente para estos equipos.

Artículo 24. La entidad designada para iniciar las pruebas a cada equipo debe solicitar al cliente la autorización emitida por la Dirección General de Comunicaciones o Dirección General de Informática, según corresponda.

Artículo 25. La entidad designada realiza, según corresponda, las acciones siguientes:

a) Verificar las características técnicas mediante mediciones a una muestra de los equipos bajo consideración, previamente evaluados por un laboratorio o instalación para la ejecución del tipo de pruebas y mediciones requeridas según el caso;

b) requerir al solicitante la información oficial del fabricante, que muestre que el equipo en cuestión cumple con las normas y parámetros establecidos;

c) requerir al solicitante el Certificado de Homologación o un documento equivalente, expedido por una autoridad competente de otro país, previamente reconocida para tales efectos, en correspondencia con el tipo de equipo en cuestión;

d) pedir al solicitante el aval procedente de una organización internacional, incluido el marcado de equipos, aplicable a determinados tipos de estos, en los casos en que este proceder haya sido previamente reconocido para dicho equipamiento;

e) tomar como referencia para las pruebas los documentos requeridos al solicitante y que previo avalúo sean reconocidos por la Dirección General de Comunicaciones o la Dirección General de Informática, según corresponda.

Artículo 26. Las pruebas realizadas por la entidad designada, deben verificar que los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación cumplen con las especificaciones técnicas establecidas en las disposiciones y normas técnicas nacionales y en ausencia de estas, con las recomendaciones internacionales reconocidas por la Dirección General de Comunicaciones o la Dirección General de Informática, según corresponda. En el proceso de verificación técnica pueden participar las entidades de control de los Órganos de la Defensa en los casos que resulten de su interés.

Artículo 27. La entidad designada elabora un informe con el resultado de las mediciones y comprobaciones técnicas realizadas a los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación bajo prueba y lo entrega al solicitante y a la Dirección General de Comunicaciones o la Dirección General de Informática, según corresponda.

Artículo 28. En el caso de equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación que por su complejidad no puedan ser evaluados técnicamente por la entidad designada para las pruebas, la Dirección General de Comunicaciones o la Dirección General de Informática, según corresponda, deciden la entrega o no del Certificado de Homologación o del documento de la evaluación

de la conformidad satisfactoria, y toman en cuenta los certificados técnicos, obtenidos del fabricante o de laboratorios extranjeros reconocidos internacionalmente y aceptados en el país. En caso de decidir que no procede emitir los documentos de aprobación, se debe informar al interesado las causas del rechazo y para ser nuevamente considerado el equipo debe demostrarse el cumplimiento de lo que origina la no aceptación.

Sección Tercera

De la Renovación del Certificado De Homologación

Artículo 29. El Certificado de Homologación tiene la vigencia que determina la instancia que lo emite que no puede ser superior a cinco años.

Artículo 30. La renovación de los certificados emitidos procede siempre que no se hayan variado sus especificaciones técnicas ni hayan sido modificados cualquiera de los datos básicos mencionados en el Artículo 18. De haberse realizado algunas de las variaciones o modificaciones antes señaladas, puede ser necesario efectuar por el interesado una nueva solicitud del Certificado de Homologación.

Artículo 31. La renovación del Certificado debe solicitarse con treinta días antes de su fecha de vencimiento. Una vez transcurrido el plazo de vigencia y no haberse gestionado la renovación, la persona jurídica que tenía el certificado no puede realizar la importación o comercialización de dicho equipo y efectúa todos los trámites para la obtención de un nuevo certificado.

CAPÍTULO IV

DE LOS CONTROLES SOBRE LOS EQUIPOS DE TELECOMUNICACIONES/TIC CERTIFICADOS

Artículo 32. Los equipos de telecomunicaciones y de Tecnologías de la Información y la Comunicación homologados están sujetos a una reevaluación, y su resultado puede implicar la cancelación del certificado en los casos siguientes:

a) Cuando se presenten ante los operadores o proveedores o ante la Dirección General de Comunicaciones, controversias, quejas, reclamos, inconformidades, que resulten ciertas, relacionados con la prestación de los servicios;

b) cuando existan indicios de que los equipos de telecomunicaciones/TIC pueden provocar afectaciones a las redes públicas y servicios de telecomunicaciones y de Tecnologías de la Información y la Comunicación, así como a la salud de las personas y al medio ambiente en general;

c) cuando como resultado de las acciones realizadas por las unidades organizativas del Ministerio de Comunicaciones facultadas para realizar el control, la inspección y la supervisión, se detecten problemas de funcionamiento, afectación de la calidad del servicio o interferencia a otros a equipos.

DÉCIMO CUARTO: El Ministerio de Comunicaciones puede realizar las inspecciones técnicas a las mercancías importadas que son reguladas por la presente resolución, a fin de verificar la autenticidad de los requisitos técnicos declarados.

DÉCIMO QUINTO: Las resoluciones vigentes emitidas por el Ministro de Comunicaciones, que hacen referencia a la obtención de los certificados de la aceptación técnica, mantienen su vigencia excepto en las partes referentes a este proceso, que es sustituido por lo que se dispone por la presente a partir de la fecha de su entrada en vigor.

DÉCIMO SEXTO: Los certificados de la aceptación técnica otorgados antes de la fecha de entrada en vigor de la presente mantienen su vigencia, para su renovación debe cumplirse lo que por la presente se dispone.

DÉCIMO SÉPTIMO: Corresponde al Director General de Comunicaciones del Ministerio de Comunicaciones elaborar el procedimiento y las medidas de control y supervisión para garantizar el cumplimiento de lo dispuesto en la presente Resolución.

DISPOSICIÓN ESPECIAL

ÚNICA: Los ministerios de las Fuerzas Armadas Revolucionarias y del Interior aseguran la conformidad de los equipos de telecomunicaciones/TIC que importen para uso militar.

DISPOSICION TRANSITORIA

ÚNICA: Para los contratos que están en ejecución al momento de entrada en vigor de la presente Resolución no le es aplicable lo dispuesto en esta.

DISPOSICION FINAL

ÚNICA: La presente Resolución entra en vigor a los sesenta días de su publicación en la Gaceta Oficial de la República de Cuba.

DESE CUENTA al Ministro del Comercio Exterior y la Inversión Extranjera y al Jefe de la Aduana General de la República.

NOTIFÍQUESE a los directores generales de Comunicaciones, de Informática, y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, a los directores de las oficinas territoriales de control del Ministerio de Comunicaciones, al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A, a los Presidentes del Grupo Empresarial de la Informática y las Comunicaciones y al de Correos de Cuba.

COMUNÍQUESE a los viceministros, a los directores generales de Defensa y de la Oficina de Seguridad para las Redes Informáticas y a los directores de Regulaciones y de Inspección del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

DADA en la Habana, a los 25 días del mes de junio del año 2019.

Jorge Luis Perdomo Di-Lella

ANEXO I RESOLUCIÓN

NOMENCLATURA DE PRODUCTOS DE IMPORTACION QUE REQUIEREN AUTORIZACION TÉCNICA DEL MINISTERIO DE COMUNICACIONES SEGÚN SACLAP VIGENTE

PARTIDAS y SUBPARTIDAS	DESCRIPCIÓN
8517	**Teléfonos, incluidos los teléfonos móviles (celulares) y los de otras redes inalámbricas; los demás aparatos para emisión, transmisión o recepción de voz, imagen u otros datos, incluidos los de comunicación en red con o sin cable (tales como redes locales (LAN) o extendidas (WAN)), distintos de los aparatos de transmisión o recepción de las partidas 84.43, 85.25, 85.27 u 85.28.**
	- Teléfonos, incluidos los teléfonos móviles (celulares) y los de otras redes inalámbricas:
8517.1100	--Teléfonos de auricular inalámbrico combinado con micrófono.
8517.1200	--Teléfonos móviles (celulares) y los de otras redes inalámbricas.(incluye teléfonos satelitales)
8517.1800	--Los demás
	- Los demás aparatos para emisión, transmisión o recepción de voz, imagen u otros datos, incluidos los de comunicación en red con o sin cable (tales como redes locales (LAN) o extendidas (WAN)):
8517.6100	-- Estaciones base
8517.6200	-- Aparatos para la recepción, conversión, emisión y transmisión o regeneración de voz, imagen u otros datos, incluidos los de conmutación y encaminamiento («switching and routing apparatus»).(Se consideran las pizarras telefónicas privadas alámbricas e inalámbricas, analógicas y digitales: PBX, PABX y WPABX, además los equipos transmisores, receptores o

	transceptores de radiocomunicaciones fijas y móviles, modem, radioenlaces y puntos de acceso inalámbrico).
8517.6900	-- Los demás. (incluye enlaces ópticos).
8517.7000	-Partes.
8518	**Micrófonos y sus soportes; altavoces (altoparlantes), incluso montados en sus cajas; auriculares, incluidos los de casco, incluso combinados con micrófono y juegos o conjuntos constituidos por un micrófono y uno o varios altavoces (altoparlantes); amplificadores eléctricos de audiofrecuencia; equipos eléctricos para amplificación de sonido.**
8518.1000	- Micrófonos y sus soportes (exclusivamente los inalámbricos).
8518.3000	-Auriculares, incluidos los de casco, estén o no combinados con micrófonos y juegos o conjunto construidos por un micrófonos y uno o varios altavoces (exclusivamente los inalámbricos)
8525	**Aparatos emisores de radiodifusión o televisión, incluso con aparato receptor o de grabación o reproducción de sonido incorporado; cámaras de televisión; cámaras digitales y videocámaras.**
8525.5000	- Aparatos emisores.
8525.6000	- Aparatos emisores con aparato receptor incorporado.(incluye equipos de control remoto para la transmisión de televisión)
8525.8000	- Cámaras de televisión, cámaras digitales y videocámaras. (exclusivamente las inalámbricas).
8526	**Aparatos de radar, radionavegación o radiotelemando.**
8526.1000	- Aparatos de radar.
	- Los demás:
8526.9100	-- Aparatos de radionavegación (incluye los aparatos de ayuda a la radionavegación).
8526.9110	--- Receptores de Sistemas de Posicionamiento por Satélites (exclusivamente los de corrección diferencial)
8526.9190	--- Los demás

8526.9200	-- Aparatos de radiotelemando.
8527	**Aparatos receptores de radiodifusión, incluso combinados en la misma envoltura con grabador o reproductor de sonido o con reloj.**
	-Aparatos receptores de radiodifusión que pueden funcionar sin fuente de energía exterior:
8527.1900	--Los demás(que difieran de los empleados comúnmente para la recepción de las bandas de radiodifusión por ondas medias, ondas cortas, frecuencia modulada o de las bandas del servicio de televisión que se presta a la población incluidos los de recepción satelital).
	-Aparatos receptores de radiodifusión que solo funcionen con fuente de energía exterior, de los tipos utilizados en vehículos automóviles:
8527.2900	-- Los demás (que difieran de los empleados comúnmente para la recepción de las bandas de radiodifusión por ondas medias, ondas cortas, frecuencia modulada o de las bandas del servicio de televisión que se presta a la población, incluidos los de recepción satelital).
8528	**Monitores y proyectores, que no incorporen aparato receptor de televisión; aparatos receptores de televisión, incluso con aparato receptor de radiodifusión o grabación o reproducción de sonido o imagen incorporado.**
	-Aparatos receptores de televisión, incluso con aparato receptor radiodifusión o grabación o reproducción de sonido o imagen incorporado:
8528.7200	--Los demás, en colores (solo los receptores de televisión digital terrestre y los receptores de televisión vía satélite)
8529	**Partes identificables como destinadas, exclusiva o principalmente, a los aparatos de las partidas 85.25 a 85.28.**
8529.1000	- Antenas y reflectores de antena de cualquier tipo; partes apropiadas para su utilización con dichos Artículos.
8531	**Aparatos eléctricos de señalización acústica o visual (por ejemplo: timbres, sirenas, tableros indicadores, avisadores**

	de protección contra robo o incendio), excepto los de las partidas 85.12 u 85.30.
8531.8000	- Los demás aparatos (exclusivamente los inalámbricos).

ANEXO II RESOLUCIÓN

NOMENCLATURA DE PRODUCTOS DE IMPORTACION SEGÚN SACLAP VIGENTE, QUE REQUIEREN AVAL TECNICO DEL COMITÉ DE COMPUTADORAS Y AUTORIZACION TÉCNICA DEL MINISTERIO DE COMUNICACIONES

PARTIDAS y SUBPARTIDAS	DESCRIPCIÓN
8443	**Máquinas y aparatos para imprimir mediante planchas, cilindros y demás elementos impresores de la partida 84.42; las demás máquinas impresoras, copiadoras y de fax, incluso combinadas entre sí; partes y accesorios:**
	- Las demás maquinas impresoras, copiadoras y de fax, incluso combinadas entre sí:
8443.3100	-- Máquinas que efectúan dos o más de las siguientes funciones: impresión, copia o fax, aptas para ser conectadas a una máquina automática para tratamiento o procesamiento de datos o a una red.
8443.3200	-- Las demás, aptas para ser conectadas a una máquina automática para tratamiento o procesamiento de datos o a una red.
8443.3900	-- Las demás.
8471	**Máquinas automáticas para tratamiento o procesamiento de datos y sus unidades; lectores magnéticos u ópticos, máquinas para registro de datos sobre soporte en forma codificada y máquinas para tratamiento o procesamiento de estos datos, no expresados ni comprendidos en otra parte.**
8471.3000	- Máquinas automáticas para tratamiento o procesamiento de datos, portátiles, de peso inferior o igual a 10 kg, que estén constituidas al menos, por una unidad central de proceso, un teclado y un visualizador.

	- Las demás máquinas automáticas para tratamiento o procesamiento de datos:
8471.4100	-- Que incluyan en la misma envoltura, al menos, una unidad central de proceso y, aunque estén combinadas, una unidad de entrada y una de salida.
8471.4900	-- Las demás presentadas en forma de sistemas.
8471.5000	- Unidades de proceso, excepto las de las subpartidas 8471.41 u 8471.49, aunque incluyan en la misma envoltura uno o dos de los tipos siguientes de unidades: unidad de memoria, unidad de entrada y unidad de salida.
8471.6000	- Unidades de entrada o salida, aunque incluyan unidades de memoria en la misma envoltura.
8471.7000	- Unidades de memoria.
8471.8000	- Las demás unidades de máquinas automáticas para tratamiento o procesamiento de datos.
8471.9000	- Los demás.
8473	**Partes y accesorios (excepto los estuches, fundas y similares) identificables como destinados, exclusiva o principalmente, a las máquinas o aparatos de las partidas 84.70 a 84.72.**
8473.3000	-Partes y accesorios de máquinas de la partida 84.71.
8473.5000	-Partes y accesorios que puedan utilizarse indistintamente con máquinas o aparatos de varias de las partidas 84.70 a 84.72.
8504	**Transformadores eléctricos, convertidores eléctricos estáticos (por ejemplo: rectificadores) y bobinas de reactancia (autoinducción).**
8504.4000	- Convertidores estáticos
8528	**Monitores y proyectores, que no incorporen aparato receptor de televisión; aparatos receptores de televisión, incluso con aparato receptor de radiodifusión o grabación o reproducción de sonido o imagen incorporado.**
	- Monitores con tubo de rayos catódicos:

8528.4200	-- Aptos para ser conectados directamente y diseñados para ser utilizados con máquinas automáticas para tratamiento o procesamiento de datos de la partida 84.71.
	- Los demás monitores:
8528.5200	-- Aptos para ser conectados directamente y diseñados para ser utilizados con máquinas automáticas para tratamiento o procesamiento de datos de la partida 84.71.
	- Proyectores:
8528.6200	-- Aptos para ser conectados directamente y diseñados para ser utilizados con máquinas automáticas para tratamiento o procesamiento de datos de la partida 84.71.
8529	**Partes identificables como destinadas, exclusiva o principalmente, a los aparatos de las partidas 85.25 a 85.28.**
8529.9000	- Las demás.

RESOLUCIÓN No. 125/2019

POR CUANTO: El Decreto 359 “Sobre el desarrollo de la Industria de Programas y Aplicaciones Informáticas” de 5 de junio de 2019 en su Disposición Final Primera establece que los jefes de los órganos y organismos del Estado y del Gobierno y entidades que correspondan, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización, y establecen las coordinaciones que resulten necesarias relativos a la aplicación del referido Decreto.

POR CUANTO: La experiencia acumulada en la aplicación de la Resolución 33 del Ministro de la Informática y las Comunicaciones, del 24 de enero del 2008, que establece el Sistema de Inscripción de Productos de Software con el propósito de ordenar los procesos de producción y comercialización en esa industria, aconsejan su actualización para atemperarla a las exigencias del proceso de informatización emprendido en el país, y es necesario emitir una nueva disposición normativa que derogue la referida disposición.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el sistema de inscripción siguiente:

SISTEMA DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

CAPÍTULO I
OBJETIVO, DEFINICIONES Y ALCANCE

Artículo 1. El objetivo del Sistema de Inscripción de los Programas y Aplicaciones Informáticas es ordenar, controlar, almacenar y mantener actualizada la información sobre estos productos existentes en el país.

Artículo 2.1. Son objeto del Sistema de Inscripción de los Programas y Aplicaciones Informáticas, en lo adelante el Sistema, los programas y aplicaciones informáticas de desarrollo y comercialización nacional, destinados a su utilización en el país o a la exportación, así como los de importación; también pueden ser objeto de inscripción a voluntad de sus desarrolladores, aquellos programas y aplicaciones informáticas que no se destinen a la comercialización o que se desarrollen con destinos específicos.

2.-Un programa y aplicación informática puede constar de varias versiones (modificaciones específicas) y cada una se inscribe.

Artículo 3. Son sujetos del Sistema las personas naturales y jurídicas, desarrolladoras y comercializadoras de programas y aplicaciones informáticas.

Artículo 4. No son objeto de inscripción los programas y aplicaciones informáticas que constituyan un software empotrado en un equipamiento tecnológico o doméstico.

Artículo 5. Los desarrolladores y comercializadores de programas y aplicaciones informáticas están obligados a inscribirlos a través de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones, en lo adelante UPTCER, previo a su comercialización.

Artículo 6. La inscripción en el Sistema no es constitutiva de derechos de propiedad intelectual sobre dichos programas y aplicaciones informáticas; la realización de este deber no es una exigencia para su posterior inscripción en el Registro de Obras Protegidas y de Actos y Contratos del Derecho de Autor.

CAPÍTULO II
DE LA SOLICITUD DE INSCRIPCIÓN

Artículo 7.1. El desarrollador o comercializador de programas y aplicaciones informáticas a través de la UPTCER, presenta a la Dirección General de Informática del Ministerio de Comunicaciones, la solicitud de inscripción en el Control Administrativo Central Interno, en lo adelante el Control, con la entrega de

los modelos A y B que se adjuntan a la presente como anexos 1 y 2, respectivamente, que incluyen las reglas para rellenarlos y que forman parte de la presente.

2. En el caso de la solicitud de inscripción por el comercializador, se presenta adicionalmente:

a) Carta del desarrollador de los programas y aplicaciones informáticas que autoriza al comercializador como representante único para la inscripción;
b) documento oficial que lo acredite para ejercer la actividad de comercialización emitido por el Ministerio correspondiente.

3. Se presenta un modelo B por cada producto que se inscribe y la certificación emitida por la dirección de la persona desarrolladora de programas y aplicaciones informáticas, o por el trabajador por cuenta propia como programador de equipos de cómputo, en el que declare la certeza sobre el funcionamiento y otros atributos del producto, a partir de las pruebas que se le hayan realizado.

4. Además, se entregan los documentos relacionados con los programas y aplicaciones informáticas regulados por las autoridades competentes siguientes:

a) El certificado para programas y aplicaciones informáticas que constituyan Sistemas Contables–Financieros, otorgados a tenor de la legislación vigente del Ministerio de Comunicaciones;
b) el certificado para programas y aplicaciones informáticas médicos, otorgadas al amparo de la legislación vigente sobre la Evaluación Estatal Sanitaria del Ministerio de Salud Pública;
c) la autorización del Ministerio de Justicia para programas y aplicaciones informáticas que gestionen las publicaciones de la Gaceta Oficial de la República.

5. De manera opcional pueden presentarse otros documentos relacionados con la calidad y avales, como el manual de usuario con la especificación de requisitos.

Artículo 8. El Ministerio de Comunicaciones puede solicitar al desarrollador o comercializador otros requisitos adicionales a lo dispuesto en la presente Resolución.

Artículo 9. El Director de la Oficina Territorial de Control, perteneciente al Ministerio de Comunicaciones, donde se detecte que se comercializa un programa y aplicación informática y no está inscrito en el Control, comunica a la autoridad competente, según corresponda, de la infracción cometida y la propuesta de medida a aplicar de acuerdo con su gravedad, para lo que tiene en cuenta las disposiciones legales vigentes en la materia.

Artículo 10. La inscripción de los programas y aplicaciones informáticas tiene una vigencia de cinco años y el productor o comercializador procede a renovarla dentro de los cuarenta y cinco días anteriores a su vencimiento; si no realiza la renovación se cancela de oficio la inscripción, y no puede comercializar el programa y aplicación informática.

Artículo 11. Los desarrolladores y comercializadores de programas y aplicaciones informáticas extranjeras tienen las mismas obligaciones que los desarrolladores y comercializadores nacionales, y cumplen lo dispuesto en la legislación vigente en cuanto a la actividad comercial.

Artículo 12. Por la inscripción del programa y aplicación informática, el desarrollador o comercializador paga cincuenta pesos; el pago se realiza directamente en la sucursal bancaria, según establece la legislación vigente del Ministerio de Finanzas y Precios, y presentan el comprobante de pago a la UPTCER, quien anexa la copia de este al expediente.

Artículo 13. Una vez presentados por el desarrollador o el comercializador los documentos que se establecen en la presente Resolución, y verificada su autenticidad, en un término de quince días, contados a partir de su presentación a la UPTCER, se le otorga la autorización por la Dirección General de Informática y la certificación de inscripción con la numeración correspondiente; este número de inscripción consta en la información de cada producto.

Artículo 14. El programa y aplicación informática puede no aceptarse o cancelarse su inscripción, de no cumplir con la legislación vigente, previa solicitud de la autoridad competente al Ministerio de Comunicaciones y se informa al desarrollador o comercializador.

CAPÍTULO III
DE LA EMISIÓN DE INFORMACIÓN

Artículo 15. La Dirección General de Informática organiza la emisión de la información sobre los programas y aplicaciones informáticas inscritas, a través del sitio web institucional del Ministerio de Comunicaciones, al que pueden acceder las personas interesadas.

Artículo 16. El sitio web institucional del Ministerio de Comunicaciones, contempla sobre los programas y aplicaciones informáticas inscritas la información siguiente:

a) Sus denominaciones y versiones y la fecha de inscripción;
b) información básica sobre el programa y aplicación informática y los certificados y avales que posea;
c) los nombres de los titulares de la inscripción, de los desarrolladores o comercializadores de programas y aplicaciones informáticas y sus datos de contacto.

SEGUNDO: Las funciones establecidas en la presente a la Dirección General de Informática, relativas a la inscripción de programas y aplicaciones informáticas se transfieren por el que suscribe a la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, una vez esta culmine su proceso de perfeccionamiento funcional, estructural y composicional.

DISPOSICIONES TRANSITORIAS

PRIMERA: Los desarrolladores o comercializadores de programas y aplicaciones informáticas que posean productos que no hayan sido inscritos y que se comercialicen, disponen para inscribirlos en el Control, de un plazo de ciento ochenta días contados a partir de la fecha de entrada en vigor de la presente Resolución.

SEGUNDA: Las inscripciones que se encuentran en trámite a la entrada en vigor de la presente Resolución, continúan este conforme con lo establecido en la legislación por la que lo comenzaron.

DISPOSICIONES FINALES

PRIMERA: El Director General de Informática del Ministerio de Comunicaciones, queda responsabilizado con la elaboración de los procedimientos necesarios internos para la implementación de lo dispuesto en la presente a partir de la fecha de su entrada en vigor.

SEGUNDA: Derogar la Resolución 33 del Ministro de la Informática y las Comunicaciones, del 24 de enero del 2008.

DESE CUENTA a los ministros del Comercio Interior y de Trabajo y Seguridad Social.

NOTIFÍQUESE al director general de informática y al Director de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y a los directores territoriales de control, pertenecientes al Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, de la Oficina de Seguridad para las Redes Informáticas y a los directores de Regulación e Inspección, pertenecientes todos al Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Dada en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella

ANEXO 1

MODELO-A DE DECLARACIÓN AL SISTEMA DE INSCRIPCIÓN DE LOS PROGRAMAS Y APLICACIONES INFORMÁTICAS

Modelo-A

DECLARACIÓN AL SISTEMA DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

(1) Denominación de la persona desarrolladora o comercializadora:

_____

Código REEUP o No. de Registro o No.de Licencia _____

(2) Nombre de la persona :

_____

(3) Dirección:

_____

_____

Teléfono: _____ **FAX**: _____ **Correo-e**: _____

(4) Línea del Programa y Aplicación Informática que desarrolla o comercializa:

_____

_____

(5) Nombre y cargo de la persona de contacto acreditada:

_____

Teléfonos: **FAX:** **Correo-e**: _____

(6) Documento presentado a la Inscripción:

_____

_____

_____

_____

Fecha de emisión de la información: _____

_____ CUÑO **Nombre y firma**

REGLAS PARA RELLENAR EL MODELO-A DECLARACIÓN AL SISTEMA DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

(1) - Denominación de la persona desarrolladora o comercializadora del software, así como su código de actividad económica REEUP, número de Registro Mercantil o número de licencia como trabajador por cuenta propia (TPCP) programador de equipos de cómputo.
(2) – Nombre de la persona que ha sido designada al frente de la organización productora o comercializadora del software o nombre del TPCP.
(3) - Dirección completa de la persona desarrolladora o comercializadora (incluir Teléfonos, FAX, correo-e y página Web).
(4) - Línea de los software que desarrolla o comercializa, tales como de gestión económica, educacional, de salud, multimedia, servicios y comercio electrónico y otros.
(5) - Nombre y cargo de la persona autorizada para suministrar la información (incluir Teléfonos, FAX y e-mail para su localización de ser necesario).
(6) - Documentos presentados a la Inscripción: Certificado Comercial expedido por el Registro Central Comercial o Licencia de Trabajador por Cuenta propia de Programador de equipos de cómputo expedido por el MTSS.

ANEXO 2

MODELO-B DE SOLICITUD DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

Modelo-B

SOLICITUD DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

(1) Denominación de la persona desarrolladora o comercializadora:

_____

_____ **Código REEUPo No. de Registroo No. de Licencia**: _____

(2) Información básica sobre el Programas y Aplicaciones Informáticas

(2.1) Denominación del Programa y Aplicación Informática:

_____

_____

(2.2) Acrónimo y versión:

_____

_____

(2.3) País de procedencia del Programa y Aplicación Informática:

_____

_____

(2.4) Breve descripción del Programa y Aplicación Informática (especificar esfera de aplicación, características, principales funcionalidades y prestaciones)**:**

_____
_____
_____
_____
_____
_____
_____

(2.5) Soporte y ayuda al cliente:

_____
_____
_____

Modelo-*B reverso*

(2.6) Relación de los documentos presentados a la Inscripción:
(Adjuntar otras hojas de ser necesario, se firman cada una de ellas)

_____
_____
_____
_____

Fecha de emisión de la información: _____

_____
Nombre y firma

(Para Uso de la Dirección General de Informática)

NÚMERO DE EXPEDIENTE:

REGLAS PARA RELLENAR EL MODELO-B DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

(1) - Denominación de la persona desarrolladora o comercializadora del software, así como su código de actividad económica REEUP, número de Registro Mercantil o número de licencia para TPCP programador de equipos de cómputo.

(2) - Información básica sobre el Programa y Aplicación Informática.

(2.1) - Denominación del Programa y Aplicación Informática: Denominación (amplia) del producto desarrollado.

(2.2) - Acrónimo y versión: Siglas o identificadores del producto de software, así como la versión del programa y aplicación informática que se comercializa. Por ejemplo: NEON v. 2.5.

(2.3) - País de procedencia del Programa y Aplicación Informática: nombre del país de donde procede el programa y aplicación informática.

(2.4) Descripción: Breve descripción de los objetivos y prestaciones que brinda el producto desarrollado, indicar esfera de aplicación, plataforma de software y hardware como características de las computadoras, mainframe, estaciones de trabajo, terminales industriales, diferentes tipos de redes sobre los cuales puede trabajar el producto (por ejemplo: Ethernet, UNIX, TCP/IP, Propietaria, Windows, UNIX u otra).

(2.5) - Soporte y ayuda al cliente: En el caso que el producto lo requiera relacionar la documentación desarrollada al efecto y el tipo de ayuda que se le brinda al cliente. (equipo de soporte técnico, visita a los clientes, ayuda en línea).

(2.6) - Relación de los documentos presentados a la Inscripción: Se relaciona toda la documentación que se adjunta a los modelos, tales como: compromiso de certidumbre sobre el funcionamiento y otros atributos del software a partir de las pruebas que se hayan realizado, el Manual de usuario, Manual para la Instalación, u otros y los certificados de cumplimiento de cuestiones legalmente establecidas como son el del MINCOM para software que constituyan Sistemas Contables– Financieros, del MINSAP para software médico y autorización del Ministerio de Justicia para programas y aplicaciones informáticas que gestionen las publicaciones de la Gaceta Oficial de la República.

RESOLUCIÓN No. 60/2019

POR CUANTO: El Acuerdo 8151 del Consejo de Ministros, del 22 de mayo de 2017, en sus numerales Cuarto y Vigésimo, apartado Primero, establece que el Ministerio de Comunicaciones tiene como funciones específicas, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de estos; así como la de proponer la política y las

estrategias para el desarrollo, evolución, producción, comercialización y utilización de las telecomunicaciones, las tecnologías de la información y la comunicación, los servicios postales, el espectro radioeléctrico, el aseguramiento técnico y de soporte asociado y, una vez aprobada, dirigir y controlar su aplicación.

POR CUANTO: El Decreto 321 del 4 de diciembre de 2013 que aprueba la Concesión Administrativa otorgada a la Empresa de Telecomunicaciones de Cuba, S.A., para la prestación de servicios públicos de telecomunicaciones, en su artículo 14 establece que el Ministerio de Comunicaciones es el encargado de aprobar los principios generales a tener en cuenta por dicha empresa en la elaboración de los contratos de los servicios concesionados, a fin de que sus cláusulas no sean abusivas y no vulneren los derechos de los consumidores.

POR CUANTO: La Resolución 197 del 21 de mayo de 2013 del Ministro de Comunicaciones, aprobó las condiciones generales de comercialización del Servicio de Acceso a Internet desde las áreas de los proveedores de Internet al público a personas naturales, la cual es necesario actualizar debido a la evolución de los servicios y en consecuencia aprobar los principios generales a tener en cuenta por la Empresa de Telecomunicaciones de Cuba, S.A., en la elaboración de los contratos correspondientes al Servicio de Acceso a Internet desde áreas públicas a personas naturales.

POR TANTO: En el ejercicio de las facultades conferidas en el Artículo 100 inciso a), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar la comercialización del Servicio de Acceso a Internet a personas naturales, en las modalidades siguientes:

1. **Cuentas temporales:** se establecen mediante la venta de tarjetas no recargables y están asociadas a la facilidad del servicio de navegación internacional.

2. **Cuentas permanentes:** se establecen mediante la firma entre el usuario que la solicite y la Empresa de Telecomunicaciones de Cuba, S.A., en lo adelante, ETECSA, del contrato que elabore la empresa a partir de los principios generales para el Servicio de Acceso a Internet ofrecido a personas naturales, que se aprueba por la presente Resolución; las facilidades de los servicios ofertados son las de navegación por la red tanto nacional como internacional y las de correo electrónico, nacional e internacional.

SEGUNDO: Aprobar los principios generales a tener en cuenta por ETECSA, en la elaboración de los contratos del servicio de acceso a Internet a personas naturales desde áreas públicas y desde el hogar, que se mencionan a continuación:

1. Habilitar las cuentas de acceso a Internet y correo electrónico de acuerdo a lo que solicite el usuario.

2. Garantizar la privacidad de los datos personales del cliente y la inviolabilidad de sus comunicaciones.
3. Establecer el sistema y el tiempo de respuesta a las reclamaciones en treinta días; para las quejas, las solicitudes de aclaración de las condiciones de prestación del servicio y las denuncias, la respuesta debe ser de forma inmediata y expedita y deben establecer e informar de las vías necesarias para cumplimentar con ello, además disponer el procedimiento de reintegro o compensación en los casos que procedan.
4. Establecer el derecho del cliente de comunicar a ETECSA cualquier inconformidad, reclamo y sugerencia con relación al servicio.
5. Establecer el sistema de comunicación al cliente, de los trabajos programados por ETECSA que puedan afectar los servicios contratados.
6. Establecer la obligación del cliente de reportar a ETECSA cualquier cambio respecto a la información relacionada con el contrato, dentro de los treinta días posteriores a su realización.
7. Garantizar la disponibilidad de los servicios, equipos y condiciones necesarias en dependencia del lugar donde se oferte el servicio.
8. Brindar información actualizada sobre las facilidades de los servicios, sus tarifas y ciclos de vida a través del portal habilitado por ETECSA y en otros medios informativos establecidos para ello así como informar cualquier modificación que puedan sufrir estas, con treinta días de antelación.
9. Atender de forma inmediata las denuncias que formule el cliente, sobre cualquier hecho fraudulento al servicio mediante el uso de sus códigos personales y contraseñas.
10. Establecer la obligación del cliente de garantizar la confidencialidad de sus códigos personales y contraseñas asociadas, a partir de que la cuenta es personal e intransferible.
11. Establecer la obligación del cliente de no ceder, revender o negociar de cualquier forma, el servicio amparado por estos principios generales.
12. Disponer la obligación del cliente de no usar el servicio para realizar acciones que puedan considerarse por ETECSA o por las autoridades administrativas y judiciales competentes, como dañinas o perjudiciales para la seguridad pública, la integridad, la ética, la moral y las buenas costumbres, la economía, la independencia y la soberanía nacional; así como actuar de acuerdo a la legislación vigente.
13. Denegar el servicio de forma inmediata cuando se detecte que el cliente ha incurrido en alguna violación de las normas de comportamiento ético establecidas, las cuales están disponibles para ser consultadas por el cliente en la ventana de autenticación; tanto la denegación de uso como las modificaciones a las normas de comportamiento ético, le son notificadas de inmediato al cliente.
14. Las partes no son responsables por el incumplimiento o cumplimiento inadecuado de sus obligaciones, cuando las mismas sean imposibles de satisfacer por causas de fuerza mayor o caso fortuito, que imposibiliten total o parcialmente su realización.
15. Brindar gratuitamente al cliente los datos estadísticos: facturación, el uso y el tráfico sobre los servicios contratados, según las peculiaridades de estos.
16. Informar las condiciones de uso del servicio con descuento de su saldo disponible y desde que el cliente se autentica se visualice el tiempo disponible en la pantalla.

17. Establecer la obligación de ETECSA, cuando el cliente está inactivo por al menos dos minutos, hacerle el cierre de sesión y notificárselo, cuando existan las condiciones técnicas para implementarlo.
18. ETECSA queda exonerada de responsabilidad civil por las limitaciones de acceso a los contenidos, la veracidad, calidad y exactitud de la información publicada en sitios Web ajenos a la empresa, así como por la pérdida de datos por el actuar del propio cliente o de terceros y la ejecución de programas malignos; asimismo, queda exonerada de los daños que el cliente pueda provocar a terceros por la ejecución de programas malignos u otras acciones.

TERCERO: Aprobar los principios generales a tener en cuenta por ETECSA en la elaboración de los contratos correspondientes al servicio de acceso a Internet a personas naturales desde áreas públicas, que se mencionan a continuación:

1. Mantener activa la cuenta de Internet, al menos por trescientos treinta días a partir del primer depósito y transcurrido ese término, queda bloqueada durante treinta días, período en el que debe recargarse, de lo contrario, la cuenta, sus datos y el saldo son cancelados, lo cual da lugar a la resolución del contrato.
2. Informar al cliente que asume el costo sobre los volúmenes de datos consumidos y la responsabilidad por las acciones realizadas por un supuesto uso fraudulento o por terceros de su cuenta de acceso, hasta tanto no solicite a ETECSA el bloqueo de esta.
3. Garantizar la privacidad y seguridad de los datos del cliente en el área de acceso a Internet al público.
4. Advertir al cliente sobre la necesidad de cambiar en la primera conexión la contraseña inicial entregada por ETECSA, para garantizar la seguridad de su cuenta.
5. Establecer la obligación del cliente de realizar el cierre de sesión al concluir su trabajo para evitar que se consuma su tiempo de conexión indebidamente.
6. Eliminar en la estación de trabajo de las áreas de Internet, cuando el terminal no pertenezca al cliente, los datos descargados o utilizados durante la sesión de forma permanente e inmediata al cierre de esta, y brindar facilidades técnicas para salvar en soportes personales la información deseada.
7. Garantizar al cliente la protección que brindan los antivirus que la empresa utiliza, y su compromiso de mantenerlos actualizados.

CUARTO: Aprobar los principios generales a tener en cuenta por ETECSA en la elaboración de los contratos correspondientes del servicio de acceso a Internet a personas naturales desde el hogar, que se mencionan a continuación:

1. Establecer que ETECSA no se responsabiliza por los daños producidos a los equipos suministrados por una inadecuada configuración o una indebida manipulación por parte del cliente.
2. Brindar los servicios con el ancho de banda y la velocidad contratada por el cliente con la calidad establecida según los indicadores vigentes.
3. Establecer la obligación de ETECSA de ofrecer al cliente asistencia técnica remota, así como la posibilidad de recibir soporte con personal técnico en los casos que lo requieran.

4. Mantener activo el acceso a Internet desde el hogar por treinta días a partir del primer depósito y transcurrido ese término, sin un nuevo depósito queda bloqueada durante treinta días, período en el que debe recargarse, de lo contrario se cancela este servicio y se bloquea el puerto de datos.
5. Establecer el sistema de comunicación anticipada al cliente, con no menos de tres días hábiles de antelación, de los trabajos programados por ETECSA que puedan afectar los servicios contratados, especificar los servicios afectados y el tiempo estimado de solución.
6. Solucionar las interrupciones asociadas al servicio, que se produzcan en la red hasta el punto de acceso a la residencia, en un término de hasta tres días, de no tener solución en este plazo, ETECSA no cobra al cliente la parte de la cuota mensual correspondiente al tiempo a partir del cual no se pudo utilizar el servicio.
7. Ejecutar las solicitudes de modificación del servicio inicialmente contratado por el cliente en los primeros siete días del mes entrante, a partir de la fecha en que se realiza la solicitud.

QUINTO: ETECSA queda encargada de comercializar el equipamiento y los accesorios necesarios para el acceso a Internet desde el hogar y no es responsable del suministro de los terminales.

SEXTO: Los contratos para el Servicio de Acceso a Internet a personas naturales conservan su validez y se actualizan por ETECSA de ser necesario, de acuerdo a lo dispuesto en la presente Resolución, en el término de hasta un año.

SÉPTIMO: Los contratos del servicio de acceso a Internet desde el hogar suscritos en la actualidad por ETECSA con sus clientes conservan su validez hasta tanto se adecuen a lo dispuesto en la presente Resolución. ETECSA dispone de un término de hasta un año a partir de la publicación de esta para realizar la adecuación y suscribir el contrato con los clientes de estos servicios, que puede ser prorrogable previa autorización del que suscribe.

OCTAVO: ETECSA remite a la dirección General de Comunicaciones y a la dirección de Regulaciones, un ejemplar de la proforma del contrato y los anexos que lo complementan, en el término de treinta días antes de su aplicación a los clientes, actualizados con los principios generales aprobados por esta Resolución.

NOVENO: ETECSA, cuando considere necesario, realiza las modificaciones a los principios generales establecidos por la presente Resolución, las somete al análisis de la dirección de Regulaciones, quien las propone a la aprobación del que suscribe.

DÉCIMO: Encargar a la Dirección General de Informática, a la Dirección de Inspección y a las Oficinas Territoriales de Control del Ministerio de Comunicaciones facultadas para realizar el control y la fiscalización según corresponda, del cumplimiento de lo dispuesto en la presente Resolución.

DÉCIMOPRIMERO: Derogar la Resolución 197 del 21 de mayo de 2013, del Ministerio de Comunicaciones.

NOTIFÍQUESE al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones y de Informática, a los directores de Regulaciones y de Inspección, y a los directores territoriales de control, del Ministerio de Comunicaciones.

ARCHÍVESE el original en la dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 21 días del mes de marzo de 2019.

Jorge Luis Perdomo Di-Lella

RESOLUCIÓN No. 320/2015

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en sus numerales Cuarto y Vigésimo, Apartado Primero, establece que el ministerio de Comunicaciones tiene la función específica de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y la implementación de los mismos; así como la de proponer la política y estrategias para la comercialización de las telecomunicaciones y la informática y una vez aprobada dirigir y controlar su aplicación.

POR CUANTO: El Decreto No. 321 "Concesión Administrativa de Servicios Públicos de Telecomunicaciones otorgada a la Empresa de Telecomunicaciones de Cuba, S.A., para la prestación de servicios públicos de telecomunicaciones", de fecha 4 de diciembre de 2013, dispone en su artículo 14, que el ministerio de Comunicaciones establece los principios generales a tener en cuenta por dicha empresa en la elaboración de los contratos de los servicios concesionados, a fin de que sus cláusulas no sean abusivas y no vulneren los derechos de los consumidores.

POR CUANTO: Mediante las resoluciones del ministro de la Informática y las Comunicaciones No. 108, de fecha 16 de junio de 2011, No. 144, de fecha 20 de septiembre de 2012 y la Instrucción No. 1, de fecha 31 de enero del 2005, emitida por el director de Regulaciones de este ministerio, fueron aprobadas las proformas del contrato general para los servicios de infocomunicaciones con sus correspondientes suplementos, la prórroga de la aplicación de dichos contratos y la proforma del contrato del servicio de transmisión de datos mediante la red de acceso por satélite VSAT, las cuales en cumplimiento de lo establecido en los fundamentos anteriores, resulta necesario derogar y en consecuencia aprobar los principios generales a tener en cuenta por la Empresa de Telecomunicaciones de Cuba, S.A., en la elaboración de los contratos correspondientes a los servicios Telemáticos y de Centro de Datos.

POR TANTO: En el ejercicio de las atribuciones conferidas en el artículo 100 inciso a), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar los principios generales a tener en cuenta por la Empresa de Telecomunicaciones de Cuba, S.A., en lo adelante ETECSA, para la contratación de los servicios Telemáticos y de Centro de Datos que se conforman por los servicios siguientes:

1. Acceso Dedicado;
2. Acceso Conmutado;
3. Acceso Asimétrico (ADSL);
4. Alojamiento de Servidores;
5. Hospedajes en servidores dedicados y virtuales;
6. Hospedajes de sitios Web y aplicaciones;
7. Plataforma pública de acceso;
8. Transmisión de Datos; y
9. Fijo por Satélite (VSAT).

SEGUNDO: Los principios generales de contratación y los que se identifican por tipo de servicio, se relacionan a continuación:

1. Principios Generales de contratación:

a) Enunciar a los clientes las causas de terminación del contrato de servicios Telemáticos y de Centro de Datos tales como: por la voluntad de las partes, que atenten contra la independencia y la soberanía nacional de la República de Cuba; el correcto ejercicio de los Servicios Telemáticos y de Centro de Datos y las telecomunicaciones en general; contra el funcionamiento de programas, equipos y sistemas informáticos, o la violación de las regulaciones relativas a la seguridad o protección de la privacidad y de los datos; los derechos sobre la propiedad intelectual e industrial de terceras personas; y las normas sobre difamación, obscenidad y demás regulaciones sobre el contenido de la información o la utilización de los servicios en actividades delictivas o que atenten contra la Seguridad Nacional y otra actividad que transgreda la legislación vigente;

b) garantizar el respeto al principio de la privacidad de los datos personales del cliente y de la inviolabilidad de sus comunicaciones;

c) enunciar a los clientes las causas de la suspensión del servicio específico contratado tales como: por no pago, o por solicitud del cliente;

d) enunciar a los clientes, las causas de la cancelación del servicio específico contratado tales como: por posesión de recursos de ETECSA sin uso después del tiempo acordado, sin pago por un tiempo determinado, por no solicitud de reconexión de un servicio más allá del tiempo de suspensión previsto, o por incumplimiento de las obligaciones que las partes asumen;

e) prestar el servicio de forma ininterrumpida, de conformidad con los indicadores de calidad aprobados por el ministro de Comunicaciones, los cuales se encuentran publicados en el sitio Web del Ministerio o de ETECSA u otros mecanismos de divulgación establecidos para la población, además disponer de un sistema de respaldo energético, que garantice la continuidad de los servicios durante las contingencias. En el caso de empleo de la tecnología de gabinetes telefónicos, este respaldo es de al menos cuatro (4) horas;

f) establecer el sistema a emplear para el reporte por los clientes de interrupciones, la demora para el restablecimiento del servicio y el procedimiento de compensación en los casos que excedan el tiempo convenido para dicho restablecimiento;

g) reconocer el derecho de los clientes de recibir información sobre la facturación oportuna y detallada del consumo del servicio facturado y establecer el procedimiento a emplear a ese fin;

h) reconocer el derecho de los clientes a utilizar los equipos terminales de su elección, siempre que no provoquen afectaciones a la red o interferencia a los servicios o violen lo establecido en la legislación vigente;

i) establecer el sistema y tiempo de respuesta a las reclamaciones en treinta (30) días; para las quejas, las solicitudes de aclaración, tanto sobre las condiciones de prestación del servicio como sobre el importe facturado y las denuncias. La respuesta debe ser de forma inmediata y expedita y deben establecer las vías necesarias para cumplimentar con ello, además disponer el procedimiento de reintegro o compensación del monto reclamado en los casos que procedan;

j) establecer el sistema de comunicación anticipada a los clientes, con no menos de tres (3) días hábiles de antelación, de los trabajos programados por ETECSA que pudieran afectar los servicios contratados, especificar los servicios que pudieran afectarse y el tiempo estimado de solución;

k) detallar los indicadores de calidad y establecer las tarifas de los servicios específicos y sus prestaciones adicionales, los cuales se encuentran publicados en el sitio Web del ministerio o de ETECSA u otros mecanismos de divulgación establecidos para la población, además incluir los servicios que integran el contrato según el tipo, la cantidad de estos, sus especificaciones y el importe que debe abonar el cliente por cada uno de ellos;

l) brindar a los clientes, los datos estadísticos sobre los servicios contratados por estos, según las peculiaridades de los mismos; y

m) establecer la obligación de los usuarios de reportar a ETECSA cualquier cambio respecto a la información relacionada con el contrato, dentro de los treinta (30) días posteriores a su realización.

2. Principios Generales por tipo de servicio:

a) Estipular un plazo para el inicio o activación de la provisión y condiciones del servicio;

b) estipular un plazo y condiciones de resolución de incidencias de los servicios (tiempo de reparación);

c) garantizar la disponibilidad de los servicios, demás equipos y condiciones necesarias;

d) informar al cliente sobre la facturación, el uso y tráfico del servicio según corresponda;

e) establecer la compensación como descuento de la cuota mensual de servicio afectado;

f) garantizar la información de la facturación en línea del mes en curso y de los últimos seis (6) meses facturados para los servicios de Accesos Dedicado y Conmutado y para este último, además la información del número de acceso;

g) garantizar el ancho de banda contratado para los servicios de Acceso Dedicado y Transmisión de Datos;

h) garantizar la calidad en la conectividad y velocidad del enlace en el servicio de alojamiento de servidores, de hospedaje en servidores dedicados y virtuales;

i) garantizar la seguridad tecnológica en los servicios de hospedaje en servidores dedicados y virtuales, en hospedaje de sitios Web o aplicaciones, transmisión de datos, acceso dedicado, conmutado, asimétrico (ADSL) y fijo por satélite (VSAT);

j) garantizar el acceso remoto desde el domicilio legal del cliente o desde una entidad en el territorio nacional que este determine y considerar como acceso nacional el enlace de gestión del servidor, para el servicio de alojamiento de servidores y de hospedaje en servidores dedicados y virtuales;

k) implementar el sistema de salva y de protección de la información del cliente para el servicio de hospedaje en servidores dedicados y virtuales y en el de Hospedaje de sitios Web o aplicaciones, y para este último en particular, garantizar los enlaces adecuados para el acceso a la Web;

l) establecer las condiciones de bloqueo inmediato del servicio ante detección de intrusos para los servicios de Acceso Dedicado, Conmutado y Asimétrico (ADSL);

m) garantizar la utilización del puerto contratado por el cliente durante las veinticuatro (24) horas de los trescientos sesenta y cinco (365) días del año para el servicio de Plataforma pública de acceso;

n) la provisión de programas actualizados que garanticen operación para el servicio de hospedaje de sitios Web o aplicaciones;

o) establecer de forma diferenciada las condiciones para:

1. los mantenimientos del equipamiento, en los servicios de alojamiento de servidores y Fijo por Satélite (VSAT);
2. las reparaciones en los servicios Fijo por Satélite (VSAT) y Transmisión de Datos; y
3. el sistema de asistencia técnica para los servicios de Hospedaje de sitios Web o aplicaciones y de acceso Asimétrico.

p) establecer sistema de cambio, periodicidad y confidencialidad de la contraseña para el servicio de Acceso conmutado, asimétrico, hospedaje en servidores dedicados y virtuales, y hospedaje de sitios Web y aplicaciones;

q) establecer sistema de notificaciones por cambios o acceso a instalaciones para los servicios de acceso asimétrico, hospedaje de sitios Web y aplicaciones y Plataforma pública de acceso; y

r) delimitar responsabilidad sobre el contenido de la información alojada por el cliente que no viole derechos ni haga daño a terceros en los servicios de Hospedaje de sitios Web y aplicaciones, hospedaje en servidores dedicados y virtuales y acceso asimétrico.

TERCERO: Los contratos se concertan de acuerdo con los principios generales, las particularidades y necesidades de los clientes y las posibilidades de ETECSA de satisfacerlo, especialmente en el caso de los órganos de la defensa.

CUARTO: Los contratos suscritos en la actualidad por ETECSA con sus clientes conservan su validez hasta tanto se adecuen a lo dispuesto en la presente Resolución. ETECSA dispone de un término de hasta dos (2) años a partir de la publicación de esta para realizar la adecuación, que puede ser prorrogable previa autorización del que suscribe.

QUINTO: ETECSA remite a las direcciones general de Comunicaciones y de Regulaciones, un (1) ejemplar de cada una de las proformas de los contratos y demás instrumentos que los complementan, actualizadas con los principios generales aprobados por esta Resolución, treinta (30) días antes de su aplicación a los usuarios.

SEXTO: ETECSA, cuando considere necesario hacer modificaciones a los principios generales establecidos por la presente Resolución, las somete a la consideración y análisis de la dirección de Regulaciones, quien las propone a la aprobación del que suscribe.

SÉPTIMO: Encargar a las unidades organizativas del ministerio de Comunicaciones facultadas para realizar el control y la fiscalización, de exigir el cumplimiento de lo dispuesto en la presente Resolución.

OCTAVO: Se derogan las resoluciones del ministro de la Informática y las Comunicaciones No. 108, de fecha 16 de junio de 2011 y No. 144, de fecha 20 de septiembre de 2012 y la Instrucción No. 1, de fecha 31 de enero del 2005, emitida por el Director de Regulaciones de este ministerio.

NOTIFÍQUESE al presidente ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones y de Informática, a los directores de Regulaciones, Inspección, Economía y a los directores territoriales de control, todos del ministerio de Comunicaciones.

ARCHÍVESE el original en la dirección Jurídica del ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 23 días del mes de diciembre de 2015.

Maimir Mesa Ramos
Ministro

RESOLUCIÓN No. 272/2015

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en su apartado Primero, numeral Decimocuarto, establece que el Ministerio de Comunicaciones tiene la función específica de proponer y una vez aprobada, regular y controlar la política para la fabricación, homologación y certificación de equipos, dispositivos, partes, accesorios, sistemas y aplicaciones en su esfera de competencia; así como proponer y establecer las regulaciones técnicas relacionadas con su importación y exportación.

POR CUANTO: La Resolución No. 10 del Ministro de la Informática y las Comunicaciones, de fecha 8 de febrero de 2006, posteriormente modificada por la Resolución No. 129, de fecha 16 de agosto de 2011, establece los equipos, partes e implementos de telecomunicaciones que las personas naturales o jurídicas pueden importar sin carácter comercial y que requieren o no autorización del Ministerio de Comunicaciones, debido al tiempo transcurrido se hace necesario actualizar este listado.

POR TANTO: En el ejercicio de las atribuciones conferidas en el Artículo 100 inciso a), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Las personas naturales o jurídicas no requieren la autorización del Ministerio de Comunicaciones para la importación sin carácter comercial de los equipos, partes e implementos de telecomunicaciones siguientes:

1. Teléfonos convencionales alámbricos y sus partes (como contestadores y accesorios diversos);
2. fax alámbricos;

3. módems destinados a la interconexión de equipos con la red telefónica;
4. teléfonos celulares (excepto los que proporcionan comunicaciones satelitales);
5. teléfonos inalámbricos, que operan en las bandas de los:

   43.710 a 49.980 MHz
   1.910 a 1.930 GHz
   2.400 a 2.4835 GHz
   5.725 a 5.875 GHz

   En los casos en que no tengan reflejada su frecuencia de trabajo pueden ser retenidos por la Aduana General de la República para su revisión por los especialistas del Ministerio de Comunicaciones y se aplican los plazos dispuestos en el apartado Tercero.

6. alarmas para vehículos;
7. alarmas contra intrusos;
8. receptores domésticos de radiodifusión (sonora en onda media, onda corta y frecuencia modulada y de televisión);
9. antenas convencionales de televisión;
10. juguetes que se accionen por radio (control remoto para juegos); y
11. micrófonos alámbricos.

SEGUNDO: Las personas naturales o jurídicas requieren de una autorización expresa de entrada al país emitida por la dirección general de Comunicaciones del Ministerio de Comunicaciones, la cual solicitan de acuerdo con los procedimientos establecidos por la legislación vigente para estos fines y que no constituye la licencia o permiso de instalación u operación, cuando estén interesadas en importar sin carácter comercial los equipos, partes e implementos de telecomunicaciones siguientes:

1. Equipos de fax inalámbricos;
2. pizarras telefónicas de todo tipo;
3. dispositivos para redes de datos “routers” (enrutadores) y “switches” (conmutadores);
4. punto de acceso inalámbricos como RLAN y otros similares, excepto WiFi que se regula por su disposición normativa específica;
5. teléfonos inalámbricos que operan en bandas diferentes a las relacionadas en el apartado Primero;
6. micrófonos inalámbricos y sus accesorios;
7. transmisores de radio de cualquier naturaleza y servicio (radares, radiofaros, radioenlaces, buscadores de personas, de radiodifusión, equipos para telemedición, telemando y otros similares);
8. transceptores de radio (equipos de estaciones fijas, móviles y personales (walkie-talkie);
9. receptores de radio profesionales, (que difieran de los aparatos domésticos de radio y televisión indicados en el apartado Primero);
10. estaciones terrenas y terminales de comunicaciones por satélites transmisoras y receptoras (incluye las estaciones receptoras de TV por satélite, las antenas parabólicas, sus accesorios y los teléfonos satelitales portátiles o de otro tipo); y

11. equipamiento destinado para la difusión masiva de datos, texto o voz por medios inalámbricos.

TERCERO: Las personas naturales o jurídicas que no presenten ante la Aduana General de la República la autorización establecida en el apartado Segundo en el caso de los equipos, partes e implementos de telecomunicaciones que corresponda, los mismos se retienen y se le otorga a la persona interesada un plazo de hasta diez (10) días, a partir de la fecha de retención, para presentar la solicitud de autorización ante la dirección general de Comunicaciones, quien debe pronunciarse sobre la misma en el transcurso de diez (10) días posteriores a la fecha de su recibo.

Si al término de treinta (30) días posteriores a la fecha de retención, no se ha presentado la debida autorización a la Aduana General de la República, esta procede conforme a lo establecido legalmente.

CUARTO: Las personas naturales o jurídicas que importen temporalmente equipos, partes e implementos de telecomunicaciones relacionados en el apartado Segundo, destinados a ferias, exposiciones y otros eventos o demostraciones similares, no requieren la obtención de la autorización, responsabilizándose el titular del régimen a quien se ha concedido la importación temporal del medio con su reexportación. El titular del régimen en caso de ser una persona jurídica puede gestionar y obtener la autorización de la dirección general de Comunicaciones para su importación definitiva, previo a la fecha de conclusión del evento, esta excepción no representa autorización para su instalación y explotación.

QUINTO: Queda prohibida la importación de equipos, dispositivos y accesorios fabricados o que se empleen para acceder sin autorización o hackear redes inalámbricas, de cualquier estándar, de detectarse se aplica lo establecido legalmente.

SEXTO: La dirección general de Comunicaciones del Ministerio de Comunicaciones es la encargada de exigir el cumplimiento de lo dispuesto en la presente Resolución.

SÉPTIMO: Derogar las resoluciones del Ministro de la Informática y las Comunicaciones No. 10, de 8 de febrero de 2006 y No. 129, de 16 de agosto de 2011, así como cualquier disposición de igual o inferior jerarquía que se oponga a la presente.

DESE CUENTA a los ministros del Interior, de las Fuerzas Armadas Revolucionarias, del Comercio Exterior y la Inversión Extranjera y al jefe de la Aduana General de la República.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones y de Informática, a los directores de Regulaciones y de Inspección; todos del Ministerio de Comunicaciones.

ARCHÍVESE el original en la dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 13 días del mes octubre de 2015.

Maimir Mesa Ramos

RESOLUCIÓN No. 140/2008

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000 cambió la denominación del Ministerio de Comunicaciones por el de Ministerio de la Informática y las Comunicaciones, para que desarrollara las tareas y funciones que realizaba el Ministerio de Comunicaciones así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sideromecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 30 de agosto del 2006, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: El Acuerdo No. 2817 de fecha 28 de noviembre de 1994, del Comité Ejecutivo del Consejo de Ministros, faculta a los Jefes de los Organismos de la Administración Central del Estado; a dictar en el límite de sus facultades y competencia, reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del organismo y, en su caso, para los demás organismos, los órganos locales del poder popular, las entidades estatales, el sector, cooperativo, mixto, privado y la población.

POR CUANTO: El Acuerdo No. 3736, de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo del Consejo de Ministros, establece que el Ministerio de la Informática y las Comunicaciones es el organismo encargado de establecer, regular y controlar la política y las estrategias para el desarrollo, la evolución, la producción, la comercialización y la utilización de los servicios y tecnologías de la informática y las comunicaciones.

POR CUANTO: El Protocolo IP versión 4 (IPv4) que opera en la actualidad las Redes Telemáticas que emplean tecnología Internet, ha sufrido cambios dados por el desarrollo de esta tecnología y su impacto en la informática y las telecomunicaciones, haciendo que este no sea eficiente por el requerimiento de nuevos servicios y la seguridad de las aplicaciones en línea. Este Protocolo está dando paso a un nuevo Protocolo IP versión 6 (IPv6) que ya esta siendo utilizado, con una generalización progresivamente a nivel mundial, dando respuesta tecnológica al desarrollo de nuevos servicios y aplicaciones basados en infraestructura IP y a la necesidad creciente de garantizar la calidad de servicio en las presentes y futuras redes que emplean la tecnología Internet.

POR CUANTO: En el país se está ordenando la introducción del Protocolo IPv6 en las Redes Telemáticas, Sistemas Informáticos y Aplicaciones de Software.

POR CUANTO: Resulta necesario establecer, para las Empresas Importadoras, Exportadoras y

Comercializadoras de productos y tecnologías que utilizan el Protocolo Internet, la exigencia de la compatibilidad de los mismos con el Protocolo IPv6 dada la responsabilidad que tienen ante sus usuarios o clientes.

POR TANTO: En el ejercicio de las facultades que me están conferidas,

RESUELVO:

PRIMERO: Establecer que las nuevas contrataciones para la importación de productos y tecnologías que utilicen el Protocolo IP, que se efectúen a partir del mes de enero del 2009, por las entidades autorizadas para ello a Nivel Nacional, tengan como exigencia principal la compatibilidad con el Protocolo IPv6

SEGUNDO: Establecer para los fabricantes de equipamiento, con interfaces de red, o que utilizan en sus diseños el Protocolo IP, realizar las modificaciones y propuestas de cambios necesarios para que sus producciones, a partir del 2 de enero del 2009, sean compatibles con el Protocolo IPv6 .

TERCERO: Las entidades comercializadoras de computadoras y equipos electrónicos que trabajen con Direcciones IP, parte activa de las Redes de Transmisión de Datos y Productos de Software, deben exigir a sus suministradores la certificación de “Productos Compatibles IPv6 ” y garantizar estas condiciones en los productos que oferten al mercado nacional.

CUARTO: Encargar a la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones la instrumentación de las medidas de control y supervisión pertinentes para garantizar el cumplimiento de lo dispuesto en la presente Resolución y a la Dirección de Regulaciones y Normas, de proponer al que resuelve, la emisión de normativas complementarias que sean necesarias para su mejor cumplimiento.

COMUNÍQUESE a los Viceministros, a los Presidentes de ETECSA, COPEXTEL, GKT y Grupo de la Electrónica, a la Dirección de Importaciones, a la Dirección de Regulaciones y Normas, a la Agencia de Control y Supervisión, al Ministerio de Comercio Exterior así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en la ciudad de La Habana, a los 6 días del mes de junio del 2008.

Ramiro Valdés Menéndez
Ministro

RESOLUCIÓN No. 49/2001

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000 cambió la denominación del Ministerio de Comunicaciones por la de Ministerio de la Informática y las Comunicaciones, que desarrollará las tareas y funciones que hasta el presente realizaba el Ministerio de Comunicaciones, así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sideromecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 12 de enero del 2000, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: De conformidad con lo establecido por el Acuerdo No. 3736 de fecha 18 de julio del 2000, adoptado por el Comité Ejecutivo del Consejo de Ministros, se dispone que el Ministerio de la Informática y las Comunicaciones (MIC) es el organismo encargado de regular, dirigir, supervisar y controlar la política del Estado y del Gobierno en cuanto a las actividades de Tecnologías Informáticas, Telecomunicaciones y Servicios de valor agregado en Infocomunicaciones.

POR CUANTO: El país lleva a cabo significativos esfuerzos para garantizar que las ventajas del comercio electrónico sean utilizadas por las entidades nacionales en función de nuestro mercado nacional e internacional.

POR CUANTO: Los avances de las tecnologías de telecomunicaciones tienen una influencia determinante en el Comercio Electrónico.

POR CUANTO: La “Concesión Administrativa del Servicio Público de Telecomunicaciones” fue otorgada mediante El Decreto No. 190, de fecha 17 de agosto de 1994, en el que se establece que el Ministerio de Comunicaciones aparte de sus funciones como organismo de la Administración Central del Estado y con el fin de asegurar la continuidad y eficaz prestación del servicio público de telecomunicaciones, es la autoridad administrativa que funge como órgano regulador de la concesión y entre sus funciones como tal, está la comprobación del cumplimiento de las condiciones que se le imponen a la Empresa de Telecomunicaciones de Cuba, S.A., en lo adelante “ETECSA” en función del interés del país.

POR TANTO: En uso de las facultades que me están conferidas

RESUELVO

PRIMERO: Disponer que la Empresa de Telecomunicaciones de Cuba S.A. (ETECSA) priorice en la utilización de la infraestructura de comunicaciones existente, en primera instancia, al conjunto de entidades que en el país suministren soluciones de comercio electrónico, sean proveedoras de estos servicios de valor agregado (comercio electrónico) ó entidades comercializadoras que utilicen para ello esta modalidad de comercio, así como las entidades de soporte asociadas, es decir, entidades

bancarias, de certificación y otras. En segundo lugar deberán ser priorizadas también las empresas que utilicen el comercio electrónico en calidad de clientes. Para lograr estos objetivos las entidades antes relacionadas deberán presentar a ETECSA la solicitud correspondiente.

SEGUNDO: Encargar a la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones la supervisión de lo dispuesto en la presente resolución.

TERCERO: Comunicar a los Viceministros, a la Dirección de Regulación y Normas, a la Agencia de Control y Supervisión, a la Empresa de Telecomunicaciones de Cuba S.A, a todos los Organismos de la Administración Central del Estado y a cuantas más personas naturales y jurídicas deban conocerla. Archivar el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones. Publicar en la Gaceta Oficial de la República de Cuba para su general conocimiento.

Dada en la ciudad de La Habana, a los 30 días del mes de marzo del 2001.

Ignacio González Planas
Ministro

REGULACIONES DEROGADAS

En el periodo comprendido entre 2020 hasta la presente publicación fueron derogadas las regulaciones siguientes:

1. Resolución No. 257/17
   Proveedores de Servicios en el Entorno Internet
2. Resolución No. 256/17
   Reglamento de Proveedor de Servicios Público de Aplicaciones
3. Resolución No. 280/2015
   Aprobación de normas del CUBANIC dominio nat.cu
4. Resolución No. 43/2013
   Dominio genérico tur y co
5. Resolución No. 220/2012
   Dominio genérico de segundo nivel gob.cu
6. Resolución No. 13/2012
   Dominio genérico cult y sld
7. Resolución No. 103/2011
   Sistema de nombres de dominios internacionalizados
8. Resolución No. 157/2008
   Nuevos dominios genéricos de segundo nivel
9. Resolución No. 150/2008
   CUBANIC genéricos
10. Resolución No. 139/2008
    Registro de los Recursos de Internet
11. Resolución No. 93/2003
    Dominios .cu en Servidores en Cuba
12. Resolución No. 92/2003
    Correo electrónico y chat internacional

ÍNDICE CRONOLÓGICO

“Desde el punto de vista político, vivimos en una época en la que hay y habrá cada vez armas más poderosas que cualquiera de las nacidas de la tecnología: las armas de la moral, la razón y las ideas. Sin ellas ninguna nación es poderosa; con ellas ningún país es débil”.

Respuesta de Fidel Castro Ruz a las declaraciones del gobierno de los Estados Unidos sobre armas biológicas, 10 de mayo de 2002

Participantes en la elaboración de los Compendios Regulatorios

Félix Emerio Garriga Sarría
Rosa Yamile García Núñez
Danilo Salvador Pérez Ordaz
Melba Pita Calderón
Wilfredo Reynaldo López Rodríguez

COMPENDIOS DE DOCUMENTOS REGULATORIOS