REPÚBLICA DE CUBA

MINISTRA DE COMUNICACIONES

RESOLUCIÓN 105

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 entidades afectadas, 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

LIC. YOANNA GARCÍA MOLINA, DIRECTORA JURÍDICA DEL MINISTERIO DE COMUNICACIONES
CERTIFICO: Que la presente Resolución es copia fiel y exacta del original que obra en los archivos de esta Dirección a mí cargo.
La Habana, 10 de agosto de 2021.

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
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
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
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
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
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	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
	2. Robo de equipamiento informático	Robo de equipamiento informático	Alto

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	2. Fallo eléctrico	Cualquier tipo de fallo eléctrico que interrumpa el funcionamiento, parcial o total, de la infraestructura TIC	Medio
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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
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
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	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
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	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
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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	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
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	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
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	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

Categoría	Subcategoría	Descripción	Nivel de Peligrosidad
	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:		