PROGRAMA SECTORIAL DE CIENCIA, TECNOLOGIA E INNOVACION

MINISTERIO DE COMUNICACIONES

FICHA DE PROGRAMA

a) **Título del Programa:** Ciberseguridad (código: PS161LH006)

b) **Prioridad**

Prioridad establecida en:

- **Lineamientos de la Política Económica y Social del Partido y la Revolución para el período 2021-2026**

84. Sustentar el avance de la Informatización de la Sociedad en un Sistema de Ciberseguridad y de gestión del espectro radioeléctrico, que fortalezca la Defensa y Seguridad Nacional. Elevar la cultura en el uso responsable de las Tecnologías de la Información y la Comunicación (TIC) por las instituciones y los ciudadanos, así como el enfrentamiento a su utilización ilegal, nociva, subversiva y desestabilizadora. Incrementar mecanismos de colaboración internacional en este campo.

- **Plan Nacional de Desarrollo económico y social hasta 2030**

(Eje estratégico: Potencial humano, ciencia, tecnología e innovación. Objetivos específicos)

11. Elevar y fortalecer la soberanía tecnológica en el desarrollo de la informática y las telecomunicaciones, así como fomentar el desarrollo de nuevas plataformas tecnológicas.

- **Política integral para el perfeccionamiento de la informatización de la sociedad en Cuba**

(Principios)

3. Instrumentar el Sistema Nacional de Seguridad Tecnológica.

c) organizar y asegurar de forma sostenida la investigación, desarrollo, asimilación tecnológica y soporte de soluciones que garanticen la seguridad de las TIC.

- **Decreto Ley No. 370 “Sobre la informatización de la sociedad en Cuba”**

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.

- **Decreto No. 360 “Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la defensa del Ciberespacio Nacional.**

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.

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.

- **Política para la Transformación Digital, la Agenda Digital Cubana y la Estrategia para el Desarrollo y Uso de la Inteligencia Artificial en el país**

- **Agenda Digital Cubana**

- **Eje 1: Marco Normativo.**

- Objetivo específico 2.3: Desarrollar el marco normativo de gestión de la ciberseguridad.

- **Eje estratégico 7: Ciberseguridad.**

- Objetivo general: Garantizar el uso responsable y seguro del Ciberespacio para que se convierta en una plataforma esencial para el progreso político, económico y social con impacto para la Seguridad Nacional y el buen funcionamiento de la Sociedad, el Estado, el Gobierno.

- **Ley 149/2022 “De Protección de Datos Personales” y Resolución 58/2022 “Reglamento para la Seguridad y Protección de los Datos Personales en Soporte Electrónico”**

- Establecen los requerimientos para la seguridad y protección de los datos personales físicos o digitales, de carácter públicos o privados en soporte electrónico.

Fundamentación:

El país se encuentra inmerso en un progresivo proceso de transformación digital de la sociedad que implica el uso seguro, ordenado y masivo de las tecnologías de la información y la comunicación (TIC). En el año 2017 el Consejo de Ministros aprobó la “Política Integral para el Perfeccionamiento de la Informatización de la Sociedad en Cuba”. La política plantea principios generales relativos a desarrollar y modernizar coherentemente todas las esferas de la sociedad, en apoyo a las prioridades del país y al ritmo de crecimiento de nuestra economía. Lo anterior se lleva a cabo bajo la premisa de avanzar en la informatización en la misma medida que se avance en la ciberseguridad del país, a partir de alcanzar soberanía y seguridad en el desarrollo y uso de las tecnologías. El Decreto No. 360/2019 del Consejo de Ministros, sobre la seguridad de las tecnologías de la información y la comunicación y la defensa del ciberespacio nacional, establece las definiciones que serán tomadas como referencia para el presente documento:

- 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.

- 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.

La Política para la transformación digital en Cuba sitúa la ciberseguridad como uno de sus ejes fundamentales y plantea que se debe garantizar el uso responsable y seguro del Ciberespacio para que se convierta en una plataforma esencial para el progreso político, económico y social con impacto para el buen funcionamiento de la Sociedad, el Estado y el Gobierno. Para ello se hace necesario aumentar la percepción de los riesgos asociados a la ciberseguridad, por las entidades y la población, así como desarrollar inversiones y soluciones tecnológicas requeridas para minimizar las vulnerabilidades de los sistemas. Para eso es necesario desarrollar competencias digitales en los ciudadanos para la adopción y uso de las tecnologías de manera crítica, segura, ética, consciente e innovadora, con un enfoque inclusivo, que contribuyan a la integración y al desarrollo pleno de la ciudadanía, en correspondencia con los valores del socialismo y la cultura nacional.

Para avanzar en la transformación digital segura de la sociedad cubana es imprescindible contar con un programa de ciencia, tecnología e innovación que permita obtener resultados superiores y sostenibles en el ámbito de la ciberseguridad. A pesar de que existen instituciones especializadas en la seguridad de las TIC, es necesario lograr mayor conexión de estas con las universidades y centros de investigación permitiendo desarrollar proyectos de I+D+i en ciberseguridad con impactos directos en el proceso de transformación digital de la sociedad.

Se han dado pasos importantes en la formación de los recursos humanos en esta temática. En las universidades se llevan a cabo programas de pregrado y posgrado relacionados con la ciberseguridad, se han introducido estas temáticas en los currículos de las carreras TIC ya existentes, así como el desarrollo de otros programas de capacitación en el sector empresarial; por lo que se han creado las condiciones para avanzar hacia la investigación en el campo de la ciberseguridad.

c) Objetivo general y específicos:

General:

Obtener resultados científicos, tecnológicos y de innovación que permitan fortalecer la ciberseguridad del país, como parte de la estrategia de transformación digital de la sociedad.

Específicos:

1. Promover investigaciones multidisciplinarias en diferentes ámbitos de la ciberseguridad que abarquen aspectos tecnológicos, organizacionales y de formación, así como la gestión de la ciberseguridad, gestión de incidentes e informática forense.
2. Potenciar la protección contra programas malignos y otras amenazas a partir del desarrollo de sistemas de ciberseguridad.
3. Realizar aportes científicos y tecnológicos en el ámbito de la criptografía, incluyendo el desarrollo de algoritmos y soluciones de infraestructuras de clave pública (PKI), entre otros aspectos.
4. Impulsar la seguridad del software, los sistemas operativos, las redes de telecomunicaciones y los dispositivos, así como la seguridad en el uso de tecnologías emergentes como el Internet de las cosas (IoT), las cadenas de bloques, la computación cuántica, la industria 4.0 entre otras.
5. Realizar aportes científicos y tecnológicos relacionados con la protección de la privacidad, la información y los datos.
6. Impulsar la protección de las infraestructuras críticas.
7. Realizar aportes a la ciberseguridad a partir de la aplicación de la inteligencia artificial y el análisis de grandes volúmenes de datos (big data).
8. Contribuir al completamiento del marco regulatorio en materia de ciberseguridad, así como a la introducción de buenas prácticas y estándares en la materia.

d) Principales resultados:

1. Se realizan propuestas que contribuyen a mejorar la gestión de los sistemas de seguridad de las TIC.
2. Los sistemas cubanos de protección contra amenazas y programas malignos evolucionan hacia soluciones más robustas.
3. Se realizan contribuciones al desarrollo de la criptografía en el país.
4. Se proponen soluciones que permiten obtener aplicaciones informáticas más seguras y fortalecer la seguridad de los sistemas operativos y las redes de telecomunicaciones.
5. La introducción de tecnologías emergentes en el país se realiza teniendo en cuenta los desafíos de ciberseguridad que implican las mismas.
6. Se avanza hacia estadios superiores en la protección de la privacidad, la información y los datos.
7. Las infraestructuras críticas cuentan con mejores sistemas de protección y ciberseguridad.

8. Se proponen soluciones que aplican técnicas de inteligencia artificial y big data para la ciberseguridad.
9. Mejora la formación y la cultura general sobre ciberseguridad.
10. Se completa el marco regulatorio y se introducen buenas prácticas y estándares en materia de ciberseguridad.

e) Indicadores verificables y medibles:

1. Publicaciones científicas relacionadas con ciberseguridad generadas en los proyectos del programa.
2. Porcentaje de los proyectos del programa que impactan directamente en el desarrollo de la ciberseguridad del país.
3. Formación de doctores y máster desde proyectos del programa.
4. Mejoras introducidas en las plataformas cubanas de protección contra amenazas y programas malignos originadas en los proyectos del programa.
5. Algoritmos y soluciones criptográficas desarrolladas en los proyectos del programa.
6. Proyectos de ciberseguridad relacionados con tecnologías emergentes.
7. Soluciones de ciberseguridad utilizando técnicas de inteligencia artificial o big data, generadas en proyectos del programa.
8. Programas de estudio, cursos y recursos educativos sobre ciberseguridad elaborados como parte de proyectos del programa.
9. Base de conocimientos a partir de realización de análisis forense a incidentes de Seguridad como parte de proyectos del programa
10. Normas desarrolladas como parte de proyectos del programa para el marco regulatorio en materia de la ciberseguridad

f) Impactos esperados:

Sociales:

Se eleva la cultura de ciberseguridad y percepción de riesgos relacionados con el empleo de las TIC.

Mejora la calidad de los servicios de gobierno y comercio electrónico a partir de contar con plataformas tecnológicas más seguras, logrando mayor bienestar social.

Se avanza de manera ordenada y segura en el proceso de transformación digital de la sociedad, contribuyendo al desarrollo sostenible del país.

Políticos:

Se mitigan los riesgos y amenazas en el ciberespacio, incluyendo la subversión política-ideológica que utiliza las plataformas tecnológicas para estos fines. Se contribuye a la estabilidad y desarrollo del sistema socialista cubano.

Científicos:

Se fomenta la investigación e innovación para el desarrollo económico – social del país, mejorando la integración entre la academia y la industria.

Económicos:

Se evitan las pérdidas por incidentes de seguridad asociados a las TIC que pueden causar daños a los sectores productivos y de servicios, especialmente a las infraestructuras críticas del país.

Avanza, de manera ordenada y segura, el proceso de transformación digital de la sociedad, lo cual permite desarrollar procesos con mayor eficiencia en todos los sectores.

Tecnológicos:

Se alcanzan niveles superiores de soberanía tecnológica en el país a partir del uso de soluciones cubanas, tecnologías libres y sistemas de código abierto.

El desarrollo tecnológico del país se produce de manera segura, propiciando el correcto avance del proceso de transformación digital de la sociedad.

Se elevan los niveles de ciberseguridad del país.

g) Entidades participantes:

Entidades del MINCOM, MININT y MINFAR a partir del encargo estatal de coordinar esta actividad en el país. Universidades, centros de estudio, entidades de ciencia, tecnología e innovación, empresas relacionadas con las TIC, parques científicos y tecnológicos, Unión de Informáticos de Cuba, formas no estatales de gestión que aborden la temática de ciberseguridad, entre otros.

h) Potencial humano y de infraestructura:

Los recursos humanos requeridos para el desarrollo de este programa existen en todo el territorio nacional, considerando los profesionales graduados de las carreras relacionadas con las TIC y otras que permitirán un enfoque multidisciplinario de las investigaciones e innovaciones. Especialmente se pueden destacar los profesionales de las universidades del MES, así como del MINCOM, MINFAR, MININT y de empresas especializadas en ciberseguridad.

Existen condiciones de infraestructura, pero deberá destinarse recursos del programa para el desarrollo y fortalecimiento de la misma que permitan la obtención de resultados en los proyectos.

i) Entidad que gestiona el programa: SEGURMATICA, Empresa de Consultoría y Seguridad Informática del Grupo Empresarial de la Informática y las Comunicaciones (GEIC).

j) Jefe del programa:

Dr.C. Mónica Peña Casanova

Graduada de Ingeniera en Telecomunicaciones en la Universidad Tecnológica de La Habana (CUJAE) en 1997, de Máster en Telemática por misma institución. Diplomada en Gestión Empresarial, Dirección Estratégica para Instituciones de Educación Superior y Administración Pública por la Universidad de La Habana. Doctora en Ciencias Técnicas por la Universidad de las Ciencias Informáticas en 2020. Profesora Titular. Miembro de las comisiones nacionales de carrera de Ingeniería en Ciencias Informática, Ingeniería en Ciberseguridad y del Programa de Formación del Nivel de Educación Superior de Ciclo Corto Administración de Redes y Seguridad Informática. Miembro de los comités académicos del Doctorado en

Telecomunicaciones de la CUJAE y la Especialidad de Postgrado en Seguridad Informática y del claustro de las maestrías de Telemática en la CUJAE, de Informática Avanzada en la UCI y del Programa Doctoral en Informática de la UCI. Actualmente se desempeña como decana de la Facultad 2 de la Universidad de las Ciencias Informáticas. Es miembro de Consejo Técnico Asesor del Grupo Empresarial de la Informática y las Comunicaciones. Sus áreas de investigación están relacionadas con la gestión de infraestructuras TI. Fue Directora de Informática del MINCOM entre 2003 y 2010. Ha participado en varios eventos científicos internacionales y ha publicado resultados de investigación en diferentes temáticas relacionadas las infraestructuras TI.

Correo electrónico: monica@uci.cu

k) Secretaria ejecutiva del programa:

Esp. Yolanda de los Angeles Varela Paez

Graduada de Ingeniera en Ciencias Informáticas en el año 2013 en la Universidad de las Ciencias Informáticas (UCI). Actualmente es la Especialista Principal del Grupo Motor Antivirus de la Empresa SEGURMATICA. Obtuvo el grado académico de Especialista de Posgrado en Seguridad Informática en el 2022. Diplomada en Gestión Empresarial en PREGER. Ha participado en eventos científicos nacionales e internacionales de temáticas relacionadas con la ciberseguridad.

Correo electrónico: yavarela@segurmatica.cu

l) Miembros del Grupo de Expertos:

1. Lic. Ingrid Barinaga Posada, Directora de Contabilidad y Finanzas, SEGURMATICA.
2. MSc. Henry Raúl González Brito, Coordinador de la Especialidad de posgrado en Seguridad Informática, UCI.
3. MSc. Antonio Hernández Domínguez, Vicedecano de Economía y Administración de la Facultad 2 de la UCI.

4. Dr.C Iván Santana Ching, Jefe de Departamento Automática FIE, UCLV.
5. MSc. David Ricardo Ledo Baster, Universidad de Holguín.
6. Lic. Juan Miguel Alonso Torres, Director de Desarrollo, SEGURMATICA
7. Dr.C. Osvaldo Andrés Pérez García, Director UEB Desarrollo de Software, CITMATEL.
8. MSc. Lauro Ramón Gattorno Rodriguez, Especialista superior TICAEST en la Dirección de Seguridad Informática, Desoft
9. Yudislay Rodríguez Calderín, Especialista Superior en Política, Dirección Jurídica del MINCOM.
10. Esp. Yohandra Echevarria Castillo, Metodóloga, UCI
11. Ing. Omar Luis Garrido Jimenez, Jefe de Departamento, UCI

m) Cantidad estimada de Proyectos: 5

n) Plazos de ejecución: 5 años

o) Presupuesto:

Años/Total	Moneda Nacional
2026	10 000 000
2027	10 000 000
2028	10 000 000
2029	10 000 000
2030	10 000 000
Total	50 000 000

p) Clientes, beneficiarios y usuarios:

- Clientes: Todos los OACE, especialmente MINCOM, MINFAR y MININT; el sistema empresarial, así como los órganos del Poder Popular, tanto a nivel central como territorial
- Beneficiarios: Toda la sociedad y la economía, ya que la ciberseguridad impacta directamente en cualquier persona natural o jurídica que haga uso de las TIC, e indirectamente en todos los que se beneficien de un servicio cuya gestión dependa de la tecnología. En función de los proyectos que se aprueben, los beneficiarios directos serán las entidades de los sectores donde se apliquen las soluciones, pero al haber proyectos transversales, pueden llegar a todos.
- Usuarios: También en función del tipo de proyecto de que se trate, los usuarios podrán ser el personal que trabaje en las organizaciones del estado o el gobierno donde se implanten las soluciones o abarcar toda la población.