PROGRAMA SECTORIAL DE CIENCIA, TECNOLOGIA E INNOVACION

MINISTERIO DE COMUNICACIONES

FICHA DE PROGRAMA

a) Título del Programa: Ciberseguridad (código: PS 161 LH 003)

b) Prioridad

Prioridad Nacional establecida en:

- **Lineamientos de la Política Económica y Social del Partido y la Revolución para el período 2016-2021**

  108. Avanzar gradualmente, según lo permitan las posibilidades económicas, en el proceso de informatización de la sociedad, el desarrollo de la infraestructura de telecomunicaciones y la industria de aplicaciones y servicios informáticos. Sustentar este avance en un sistema de ciberseguridad que proteja nuestra soberanía tecnológica y asegure el enfrentamiento al uso ilegal de las tecnologías de la información y la comunicación. Instrumentar 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.

c) Fundamentación:

El país se encuentra inmerso en un progresivo proceso de informatización 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 un grupo de 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 un grupo de 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.

Para avanzar en la ciberseguridad del país es imprescindible contar con un programa de ciencia, tecnología e innovación que permita obtener resultados superiores y sostenibles. A pesar de que existen un grupo de instituciones especializadas en la seguridad de las TIC, es necesario lograr una mayor conexión de estas con las universidades y centros de investigación que permita desarrollar proyectos de I+D+i en ciberseguridad con impactos directos en la seguridad nacional y el proceso de informatización.

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, así como se desarrollan otros programas de capacitación en el sector empresarial; por lo que se van creando las condiciones para avanzar hacia la investigación en el campo de la seguridad de las TIC.

d) Objetivos general y específicos:

General:

Obtener resultados científicos, tecnológicos y de innovación que permitan fortalecer la ciberseguridad del país, como parte de la estrategia de informatización, a partir del desarrollo de proyectos de investigación el campo de la seguridad de las TIC.

Específicos:

1. Promover investigaciones multidisciplinarias en diferentes ámbitos de la ciberseguridad que abarquen aspectos tecnológicos, organizacionales y de formación del capital humano.
2. Contribuir a mejorar la protección contra programas malignos y otras amenazas a partir del desarrollo de plataformas de ciberseguridad y sistemas antimalware cubanos.
3. Realizar aportes científicos y tecnológicos en el ámbito de la criptografía, lo cual incluye el desarrollo de algoritmos y soluciones de infraestructuras de clave pública (PKI), entre otros aspectos.
4. Impulsar el desarrollo de investigaciones e innovaciones para la seguridad del software, los sistemas operativos, las redes de telecomunicaciones y los dispositivos móviles.
5. Realizar investigaciones relacionadas con la protección de la privacidad y datos personales.
6. Contribuir a mejorar la protección de las infraestructuras críticas a partir del desarrollo de proyectos que aborden esta temática.
7. Desarrollar investigaciones sobre seguridad en tecnologías emergentes como: Internet de las cosas (IoT), cadenas de bloques, computación cuántica, industria 4.0, entre otras.
8. Realizar aportes a la ciberseguridad a partir de la aplicación de técnicas de inteligencia artificial y análisis de grandes volúmenes de datos (big data).
9. Promover el desarrollo de proyectos en el campo de la gestión de la ciberseguridad, gestión de incidentes e informática forense.
10. Impulsar el desarrollo de iniciativas para la formación en ciberseguridad que abarquen el diseño de programas de posgrado y pregrado, así como recursos educativos y otras propuestas para elevar la cultura de ciberseguridad de la población.

e) Principales resultados:

1. Se ejecutan proyectos de I+D+i en diferentes ámbitos de la ciberseguridad que que impactan en el desarrollo de esta temática en el país.
2. Evolucionan hacia soluciones más robustas las plataformas cubanas de protección contra amenazas y programas malignos.
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. Se avanza hacia estadios superiores en la protección de la privacidad y datos personales.
6. Las infraestructuras críticas cuentan con mejores sistemas de protección y ciberseguridad.
7. La introducción de tecnologías emergentes en el país se realiza teniendo en cuenta los desafíos de ciberseguridad que implican las mismas.
8. Se proponen soluciones que aplican técnicas de inteligencia artificial y big data para la ciberseguridad.
9. Se realizan propuestas que contribuyen a mejorar la gestión de los sistemas de seguridad de las TIC de las instituciones.
10. Mejora la formación en ciberseguridad y la cultura general de la población en esta temática.

f) Indicadores verificables y medibles:

1. Publicaciones científicas relacionadas con ciberseguridad.
2. Porciento de los proyectos del programa que impactan directamente en el desarrollo de la ciberseguridad del país.
3. Mejoras introducidas en las plataformas cubanas de protección contra amenazas y programas malignos.
4. Algoritmos y soluciones criptográficas desarrolladas.
5. Resultados de los controles de seguridad realizados a las instituciones, aplicaciones informáticas y redes de telecomunicaciones.
6. Incidentes de seguridad en infraestructuras críticas.
7. Proyectos de ciberseguridad relacionados con tecnologías emergentes.
8. Soluciones de ciberseguridad que apliquen técnicas de inteligencia artifical o big data.
9. Programas de estudio, cursos y recursos educativos sobre ciberseguridad.
10. Cultura general de población en aspectos de ciberseguridad.

g) Impactos esperados:

Sociales:
La población eleva su 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 un mayor bienestar social.
Se avanza de manera ordenada y segura en el proceso de informatización del país, contribuyendo al desarrollo sostenible de la sociedad.

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, así como a la preservación de la seguridad nacional.

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, y muy especialmente a las infraestructuras críticas del país.
Avanza, de manera ordenada y segura, el proceso de informatización, lo cual permite desarrollar procesos con mayor eficiencia en todos los sectores de la economía.

Tecnológicos:
Se alcanzan niveles superiores en la 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 informatización de la sociedad.
Se elevan los niveles de ciberseguridad del país.

h) 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 se aborden la temática de ciberseguridad, entre otros.

i) 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 deberán destinarse un grupo de recursos del programa para el desarrollo y fortalecimiento de las mismas que permitan la obtención de resultados en los proyectos.

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

k) Jefe del Programa:

Dr.C. Raydel Montesino Perurena
Graduado de Ingeniero en Telecomunicaciones y Electrónica en el año 2003 en la Universidad Tecnológica de la Habana (CUJAE). Actualmente es Vicerrector Primero y Profesor Titular de la Universidad de las Ciencias Informáticas (UCI). En este centro además ocupó las responsabilidades de Director de Redes y Seguridad Informática (2005 - 2013) y Vicerrector de Tecnología (2013 - 2015). Obtuvo el grado científico de Doctor en Ciencias Técnicas en el año 2013. Cursó la Especialidad en Seguridad y Defensa Nacional del Colegio de Defensa Nacional (CODEN) en el año 2016. Ha participado en varios eventos científicos nacionales e internacionales y ha publicado resultados de investigación en diferentes temáticas relacionadas con la ciberseguridad, específicamente en lo referente a estándares, indicadores, automatización de controles y sistemas de gestión de información y eventos de seguridad (SIEM).
Email: raydelmp@uci.cu

l) Secretario Ejecutivo del Programa:

Ing. 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 especialista de la Empresa de Consultoría y Seguridad Informática SEGURMATICA, donde ocupa la responsabilidad de coordinadora del grupo de desarrollo del motor antivirus. Posee certificaciones profesionales que avalan su preparación en ciberseguridad y ha participado en varios eventos científicos nacionales e internacionales en estas temáticas.
Email: yavarela@segurmatica.cu

m) Miembros del Grupo de Expertos:

1. MSc. Miguel Gutiérrez Rodríguez, Dirección General de Informática, MINCOM.
2. Ing. Pablo Domínguez Vázquez, Dirección de Ciberseguridad, MINCOM.
3. Dr.C. Jesús Alejandro Santos Reyes, Dirección de Tecnologías y Sistemas, MININT.
4. MSc. Miriam Rosado Martínez, Dirección de Tecnologías y Sistemas, MININT.
5. Dr.C. Pablo Freyre Arrozarena, Centro de Ciencia y Tecnologías Criptográficas, MININT.
6. MSc. Darío Dominicis Bravo, Departamento de Informática y Cifras, MINFAR
7. MSc. Aisel Guerrero Luis, Centro de Ciberseguridad, MINFAR
8. Ing. Daniel Ramos Fernández, Dirección de Operaciones de Seguridad, ETECSA.
9. Ing. Michell Rodriguez Averoff, Dirección de Operaciones de Seguridad, ETECSA.
10. MSc. Gonzalo García Pierrat, Especialista principal, OSRI.
11. Dr.C. Walter Baluja García, Rector, UCI.
12. Dr.C. Yanio Hernández Heredia, Vicerrector, UCI.
13. Dra.C. Oristela Cuellas Justi, Vicedecana, UCI.
14. MSc. Henry Raúl González Brito, Coordinador de la Especialidad de posgrado en Seguridad Informática, UCI.
15. Ing. Darvis Dorvigny Dorvigny, Director de Seguridad Informática, UCI.
16. MSc. Antonio Hernández Domínguez, Director del Centro de Telemática, UCI.
17. MSc. José Cuza Freire, Universidad de Oriente.
18. MSc. Ernesto Rodríguez Fernández, Universidad de Oriente.
19. Dr.C Iván Santana Ching, Departamento Automática FIE, UCLV.
20. Dr.C. Roberto Sepúlveda Lima, MES.
21. Dr.C. Humberto Díaz Pando, Decano, CUJAE.

22. Ing. Yanser Falcón Alonso, Universidad de Matanzas.
23. Dra.C. Teresa B. López Pagés, Instituto de Criptografía, Universidad de la Habana.
24. MSc. José Rodríguez, Instituto de Criptografía, Universidad de la Habana
25. MSc. Evaristo J. Madarro Capó, Instituto de Criptografía, Universidad de la Habana.
26. MSc. David Ricardo Ledo Blaster, Universidad de Holguín.
27. MSc. Juan Miguel Alonso Torres, SEGURMATICA
28. Dr.C. Osvaldo Andrés Pérez García, CITMATEL.
29. MSc. Lauro Ramón Gattorno Rodriguez, Dirección General de Defensa, MINCOM
30. MSc. José Manuel Santos, DDT, MINCOM.

n) Cantidad estimada de Proyectos: 10

o) Plazos de ejecución: 4 años

p) Presupuesto:

Años/Total	Moneda Nacional	Divisas
2022	8 000 000	250 000
2023	8 000 000	250 000
2024	7 000 000	200 000
2025	7 000 000	200 000
Total	**30 000 000**	**900 000**

q) 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.