PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 259.-

POR LA CUAL SE APRUEBA LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2025-2028.-

- 1 -

Asunción, mayo de 2025

VISTO: *La actuación de fecha 19 de mayo de 2025, por la cual la Dirección de Gabinete del Ministerio de Tecnologías de la Información y Comunicación, otorga el visto bueno correspondiente para la aprobación por resolución ministerial de la propuesta de la Estrategia Nacional de Ciberseguridad 2025-2028; el Expediente Digitalia N° 2024-12021001-008782, y,----------*

CONSIDERANDO: *Que, la Ley Nº 6207/2018 “QUE CREA EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y ESTABLECE SU CARTA ORGÁNICA”, en su Artículo 8º, establece que el Ministro es la máxima autoridad institucional. En tal carácter es el responsable de la dirección y gestión especializada, técnica, financiera y administrativa de la Entidad, en el ámbito de sus atribuciones legales, asimismo, ejerce la representación legal del Ministerio. Además, en su Artículo 2° dispone que: “El Ministerio es un órgano del Poder Ejecutivo, de derecho público. Se constituye en la entidad técnica e instancia rectora, normativa, estratégica y de gestión especializada, para formulación de políticas e implementación de planes y proyectos en el ámbito de las Tecnologías de la Información y Comunicación en el sector público, y de la comunicación del Poder Ejecutivo tanto en su aspecto social como educativo para la inclusión, apropiación e innovación en la creación, uso e implementación de las tecnologías.”.----------*

Que, en idéntico sentido, el Decreto N° 2274/2019, por el cual se reglamenta la Ley citada, establece que el MITIC es la autoridad nacional en materia de ciberseguridad, asumiendo el papel central en la protección del ecosistema digital, con facultades que abarcan desde la prevención y control de incidentes cibernéticos hasta la formulación de políticas y normativas; planes y estrategias nacionales relacionados con la ciberseguridad.----------

Que, el Ministerio de Tecnologías de la Información y Comunicación (MITIC) es el organismo responsable de coordinar la ejecución de acciones conjuntas e integradas entre las distintas entidades del sector público en áreas clave como la ciberseguridad. Asimismo, en este ámbito el MITIC tiene la facultad de diseñar, coordinar y monitorear políticas públicas, planes y estrategias que deben ser implementadas por los OEE, asegurando la protección de los sistemas digitales gubernamentales y la información sensible del Estado.-

Que, el MITIC desempeña un rol fundamental en la formulación, asesoramiento y regulación de políticas nacionales en materia de protección de datos personales y gubernamentales, así como en la promoción del uso de tecnologías en la educación y en la consolidación de un entorno digital seguro. En este sentido, ejerce como la Autoridad Nacional de Ciberseguridad, con la responsabilidad de prevenir, gestionar y controlar incidentes cibernéticos que representen una amenaza para el ecosistema digital del país, estableciendo mecanismos de respuesta y fortaleciendo la resiliencia cibernética a nivel nacional.----------

Que por actuación de fecha 18 de febrero de 2025, el Viceministerio de Tecnología de la Información y Comunicación eleva a consideración de la Máxima Autoridad de la institución la propuesta de Estrategia Nacional de Ciberseguridad 2025-2028 para su aprobación por resolución ministerial.----------

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 259.-

POR LA CUAL SE APRUEBA LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2025-2028.-

Que por Dictamen DGAJ N° 25 de fecha 11 de marzo de 2025, la Dirección General de Asesoría Jurídica, en su parte conclusiva, recomienda la aprobación de la Estrategia Nacional de Ciberseguridad, estableciendo que la misma se encuentra enmarcada dentro de las competencias del Ministerio de Tecnologías de la Información y Comunicación (MITIC), conforme a lo dispuesto en la Ley N° 6207/2018. Asimismo, sugiere elevar la Estrategia al Poder Ejecutivo para su aprobación mediante Decreto, y abrogar el Decreto N° 7052/2017. Finalmente, propone diferir la conformación de la Comisión Nacional de Ciberseguridad y sus subcomités hasta tanto se reestructure el Sistema Nacional de Ciberseguridad y se definan los ajustes necesarios conforme al nuevo contexto nacional.--

POR TANTO, *en ejercicio de sus atribuciones legales,----------*

EL MINISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN,

R E S U E L V E:

Artículo 1º.- ***Aprobar*** *la Estrategia Nacional de Ciberseguridad para el periodo 2025-2028, en reemplazo del Plan Nacional de Ciberseguridad (2017), que como Anexo forma parte integrante de la presente Resolución.----------*

Artículo 2º.- ***Designar*** *al Director General de Ciberseguridad y Protección de la Información como Coordinador Nacional de Ciberseguridad. ----------*

Artículo 3º.- ***Abrogar*** *la Resolución MITIC N° 032/2024 “POR LA CUAL SE DESIGNA COMO COORDINADOR NACIONAL DE CIBERSEGURIDAD AL SR. JORGE ANDRÉS LEVERA GÓMEZ, DIRECTOR GENERAL DE CIBERSEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN DEL VICEMINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE ESTA CARTERA DE ESTADO”.----------*

Artículo 4º.- ***Elevar*** *la Estrategia Nacional de Ciberseguridad (ENC) 2025-2028 al Poder Ejecutivo para su aprobación mediante decreto y disponer en consecuencia la abrogación del Decreto N° 7052/2017.-*

Artículo 5º.- *La presente Resolución entrará en vigencia a partir de la fecha de su firma por parte de la máxima autoridad de la institución.----------*

Artículo 6º.- *La presente Resolución será refrendada por la Secretaria General de la Institución.----------*

Artículo 7º. ***Comunicar*** *a quienes corresponda, y cumplido, archivar. ----------*

MARIA CONCEPCION RIVAS LAGUARDIA
Firmado digitalmente por MARIA CONCEPCION RIVAS LAGUARDIA
Fecha: 2025.05.19 14:31:49 -03'00'
Secretaria General

GUSTAVO EMIGDIO VILLATE SAMANIEGO
Digitally signed by GUSTAVO EMIGDIO VILLATE SAMANIEGO
Date: 2025.05.19 14:25:30 -03'00'
Ministro

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

2025-2028

GOBIERNO DEL PARAGUAY | MITIC

CERT-PY

La ciberseguridad no es solo un tema técnico. Su impacto abarca todas las funciones de un país y requiere una estrategia integral centrada en las personas, involucrando a actores de los sectores público y privado, la academia, la sociedad civil, pilares fundamentales para la seguridad nacional.

La rápida digitalización y el avance de tecnologías emergentes plantea desafíos críticos en materia de ciberseguridad. La protección de infraestructuras esenciales depende de estrategias efectivas, y una cultura de prevención, que mitiguen las vulnerabilidades inherentes a la digitalización para garantizar su continuidad. También, es urgente abordar la brecha de talento en ciberseguridad, ya que la demanda de profesionales especializados sigue creciendo. Esto permite fortalecer la capacidad de respuesta ante amenazas digitales.

La Estrategia Nacional de Ciberseguridad 2025-2028, actualiza el Plan Nacional de Ciberseguridad 2017 y establece la posición del Paraguay y sus prioridades estratégicas para mejorar los niveles de madurez en ciberseguridad y fortalecer la protección del país frente a las múltiples amenazas digitales para los próximos cuatro años.

La ciberseguridad necesita de trabajo en equipo, compartir conocimientos y experiencias para mejorar continuamente. Esta estrategia fue construida durante el 2024, tomando como base estándares internacionales adaptados a la realidad nacional. El proceso de actualización se realizó en etapas, con un diagnóstico inicial, entrevistas, mesas de diálogo presenciales y virtuales, plataformas de participación, consultas públicas con la participación de más de 500 participantes en las etapas del proceso, profesionales y ciudadanos de todo el ecosistema de ciberseguridad nacional, quienes compartieron sus visiones, puntos de vista y observaciones a la propuesta, plasmadas en la Estrategia. Además, esta estrategia contiene una hoja de ruta para su implementación, que incluye líneas de acción de Instituciones de Gobierno, que buscan mejorar la resiliencia ante las ciberamenazas, proteger la infraestructura crítica y fortalecer la ciberseguridad, con metas centradas en las personas.

La cooperación internacional, a través de la Organización de Estados Americanos, y todos los organismos externos que participaron del proceso, han demostrado ser fundamentales, permitiendo al país tener la visión más allá de las fronteras, a nivel mundial y regional, así como sus opiniones y experiencias como expertos en la materia.

Hoy reafirmamos el compromiso del gobierno en fortalecer la ciberseguridad como un pilar fundamental para el desarrollo nacional. Doy un agradecimiento especial a todos quienes participaron por su tiempo, su dedicación, predisposición y aportes. Juntos, construimos un entorno digital más seguro y resiliente para enfrentar los desafíos actuales y futuros.

Gustavo Villate, Ministro
Ministerio de Tecnologías de la Información y Comunicación - MITIC

GOBIERNO DE LA REPÚBLICA DE PARAGUAY

Santiago Peña
Presidente de la República

Gustavo Villate
Ministro de Tecnologías de la Información y Comunicación -MITIC-

Klaus Pistilli
Viceministro de Tecnologías de la Información y Comunicación -MITIC-

Pedro Martínez
Director General de Ciberseguridad y Protección de la Información -MITIC-

Diana Valdez
Directora de Centro de Respuestas ante Incidentes Cibernéticos de Paraguay (CERT-PY)

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

Luis Almagro
Secretario General

Iván Marques
Secretario de Seguridad Multidimensional -SMS-

Alison August Treppel
Secretaria Ejecutiva
Comité Interamericano contra el Terrorismo -CICTE-

Kerry-Ann Barrett
Orlando Garcés
David Moreno
Sección de Ciberseguridad

RESUMEN EJECUTIVO

En la era digital actual, la ciberseguridad se ha convertido en un pilar fundamental para el desarrollo sostenible y la prosperidad de las naciones. Paraguay, reconociendo esta realidad, ha dado pasos significativos en la consolidación de su ecosistema de ciberseguridad desde la implementación de su Plan Nacional de Ciberseguridad 2017. Sin embargo, el panorama de amenazas cibernéticas evoluciona constantemente, presentando nuevos desafíos que requieren una respuesta integral y adaptativa. En este contexto, la Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay se presenta como una hoja de ruta actualizada y ambiciosa para fortalecer la resiliencia digital del país.

Esta estrategia se construye sobre los logros alcanzados y las lecciones aprendidas del plan anterior, al tiempo que incorpora las mejores prácticas internacionales y se alinea con los estándares globales de ciberseguridad. Se ha desarrollado mediante un proceso inclusivo y participativo, involucrando a múltiples partes interesadas del ecosistema digital paraguayo, incluyendo entidades gubernamentales, sector privado, academia y sociedad civil. Este enfoque colaborativo asegura que la estrategia refleje las necesidades y aspiraciones de todos los sectores de la sociedad paraguaya.

La Estrategia Nacional de Ciberseguridad 2025-2028 se fundamenta en principios clave como la gobernanza efectiva, la gestión integral de riesgos, la cooperación nacional e internacional, y la responsabilidad compartida. Adopta un enfoque centrado en el ser humano, promoviendo la equidad en el acceso a herramientas y formación en ciberseguridad, con especial atención a grupos vulnerables. Además, fomenta la innovación y la adopción segura de tecnologías emergentes como pilares para fortalecer las capacidades de defensa y respuesta del país ante amenazas cibernéticas.

Los objetivos estratégicos de esta iniciativa abarcan áreas críticas como el fortalecimiento del marco legal y regulatorio, la protección de infraestructuras críticas, el desarrollo de capacidades técnicas y humanas, la promoción de una cultura de ciberseguridad, y el impulso a la cooperación internacional. La estrategia también pone énfasis en la sostenibilidad de las iniciativas propuestas, buscando desarrollar capacidades locales duraderas y establecer mecanismos de financiamiento que aseguren la continuidad de los esfuerzos en ciberseguridad a largo plazo.

Al implementar esta estrategia, Paraguay se posiciona para enfrentar los desafíos cibernéticos del futuro, protegiendo los intereses nacionales y fomentando un ciberespacio seguro y confiable para todos sus ciudadanos. Este documento contó con el apoyo técnico especializado de la Sección de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA/CICTE) y representa el compromiso del país con la construcción de un ecosistema digital resiliente, que no solo proteja contra las amenazas actuales, sino que también esté preparado para adaptarse a los retos emergentes, contribuyendo así al desarrollo socioeconómico sostenible de Paraguay en la era digital.

TABLA DE CONTENIDO

LISTA DE GRÁFICAS

LISTA DE CUADROS

SIGLAS Y ACRÓNIMOS

BAM	Banda Ancha Móvil
BID	Banco Interamericano de Desarrollo
CAF	Banco de Desarrollo de América Latina
CICTE	Comité Interamericano contra el Terrorismo de la OEA
CERT-PY	Centro de Respuestas ante Incidentes Cibernéticos del Paraguay
CODENA	Consejo de Defensa Nacional del Paraguay
CONATEL	Comisión Nacional de Telecomunicaciones del Paraguay
CPP	Código Procesal Penal
CSIRT	Equipo de Respuesta a Incidentes de Seguridad Informática (en inglés, Computer Security Incident Response Team)
DevSecOps	Metodología de Desarrollo, Seguridad y Operaciones (en inglés, Development, Security, and Operations)
DGCPI	Dirección General de Ciberseguridad y Protección de la Información del MITIC
DoS	Ataque de Denegación de Servicio (en inglés, Denial-of-service attack)
DDoS	Ataque Distribuido de Denegación de Servicio (en inglés, Distributed Denial-of-Service)
FGE	Fiscalía General del Estado del Paraguay
GCI	Índice Global de Ciberseguridad de la UIT (en inglés, Global Cybersecurity Index)
HW	Componente físico de un sistema informático (en inglés, Hardware)
IA	Inteligencia Artificial
IICN	Infraestructuras de Información Críticas Nacionales
INE	Instituto Nacional de Estadística del Paraguay
IoT	Internet de las Cosas
ISO	Organización Internacional de Normalización (en inglés, International Organization for Standardization)
I+D	Investigación y Desarrollo
LTE	Estándar móvil de Evolución a Largo Plazo (en inglés, Long Term Evolution)
MERCOSUR	Mercado Común del Sur
MITIC	Ministerio de Tecnologías de la Información y Comunicación del Paraguay
MoU	Memorandos de entendimiento (en inglés, Memorandum of Understanding)
NICE	Iniciativa Nacional para la Educación en Ciberseguridad de NIST (en inglés, National Initiative for Cybersecurity Education)
NIST	Instituto Nacional de Normas y Tecnología de Estados Unidos (en inglés, National Institute of Standards and Technology)
NCSI	Índice Nacional de Ciberseguridad del e-Governance Academy de Estonia (en inglés, National Cyber Security Index)
OEA	Organización de Estados Americanos
OEE	Organismos y Entidades del Estado
ONU	Organización de Naciones Unidas
PNTIC	Plan Nacional TIC del Paraguay
PYME	Pequeña y Mediana Empresa
SOC-PY	Centro de Operaciones de Seguridad del Paraguay (en inglés, Security Operations Center of Paraguay)
STEM	Ciencia, Tecnología, Ingeniería y Matemáticas (en inglés, science, technology, engineering, and mathematics)
SW	Componente lógico de un sistema informático (en inglés, software)
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y las Comunicaciones
UIT	Unión Internacional de Telecomunicaciones (en inglés, International Telecommunication Union)
WEF	Foro Económico Mundial (en inglés, World Economic Forum)

1. CONTEXTO INTERNACIONAL

A medida que el mundo se vuelve cada vez más interconectado[1] gracias a los avances en las Tecnologías de la Información y las Comunicaciones (TIC), el panorama de la ciberseguridad se ha vuelto aún más complejo. Las distintas regiones alrededor del mundo enfrentan desafíos y oportunidades sin precedentes.

En la última década, el acceso a las TIC y la adopción digital han aumentado significativamente, especialmente en áreas rurales y previamente desatendidas[2]. Las iniciativas de transformación digital, respaldadas por gobiernos, organizaciones multilaterales y el sector privado, han conducido a una mayor conectividad. Los esfuerzos por cerrar la brecha digital[3] han permitido que millones de personas en la región participen en la economía digital, accedan a la educación y se beneficien de servicios públicos en línea.

Con la mejora en el acceso a las TIC, ha habido una rápida afluencia de nuevos usuarios de Internet, muchos de los cuales carecen de las habilidades necesarias en alfabetización digital y ciberseguridad. Esta situación ha ampliado la superficie de ataque[4] para actores maliciosos, creando vulnerabilidades en áreas rurales donde la educación y conciencia en ciberseguridad suelen ser limitadas.

La rápida adopción de nuevas tecnologías digitales como la inteligencia artificial (IA), la cadena de bloques (blockchain) y el Internet de las Cosas (IoT) ha transformado las industrias y los servicios. Estas tecnologías ofrecen beneficios sustanciales en eficiencia, automatización y toma de decisiones, pero han introducido nuevos riesgos[5].

Los principales desafíos que enfrentan las organizaciones para mantenerse vigilantes frente a los riesgos en constante evolución incluyen la creciente sofisticación de los ataques, la explotación de vulnerabilidades de día cero, la proliferación del ransomware, las amenazas provenientes de ciertos Estados nacionales, agentes no estatales y las vulnerabilidades inherentes a los dispositivos IoT.

A pesar del creciente panorama de amenazas cibernéticas, la mayoría de los países de la región América Latina y el Caribe demuestra un compromiso básico o medio en materia de ciberseguridad con acciones impulsadas por los gobiernos que incluyen la evaluación, el establecimiento o la implementación de ciertas medidas de ciberseguridad

[1] A finales de 2023, aproximadamente el 67% de la población mundial (5,4 billones de personas) estuvieron conectadas a Internet, representando un crecimiento del 4,7% desde 2022 (ITU, 2023a).
[2] La penetración de Internet en zonas rurales en la región Américas pasó de un 68% en 2022 a un 74% en 2023 (ITU, 2022) (ITU, 2023a).
[3] La brecha digital alcanzó en el 2022 a más del 64% de la población rural de América Latina y el Caribe y el 40% de los hogares urbanos con menor quintil de ingresos (CAF, 2024)
[4] En el año 2023, FortiGuard Labs bloqueó 2,4 billones de intentos de vulnerabilidad y 3 billones de entregas de malware a nivel global (FORTINET, 2024).
[5] Entre los riesgos más urgentes relacionados con la IA se encuentra la difusión de información errónea y desinformación, considerada el riesgo global más grave previsto para los próximos dos años (WEF, 2024).

generalmente aceptadas[6]. Aún es necesario fortalecer las capacidades para prevenir, detectar y responder a incidentes cibernéticos. En muchos casos, los presupuestos de ciberseguridad son insuficientes y el personal carece de la formación y los recursos necesarios para mitigar y responder a las amenazas.

La evolución del ciberdelito continúa superando la capacidad de los marcos normativos (legales y regulatorios) y de las agencias de aplicación de la ley para investigar y procesar eficazmente a los perpetradores. Los sistemas tradicionales de justicia penal a menudo no están equipados para lidiar con la naturaleza transnacional del ciberdelito, lo que conduce a lagunas en la rendición de cuentas.

Abordar los desafíos de ciberseguridad requiere una respuesta coordinada y multinivel a nivel global, regional y local. Las naciones deben colaborar para crear estrategias de ciberseguridad resilientes, compartir inteligencia sobre amenazas y construir un enfoque integral para la gobernanza digital.

2. CONTEXTO NACIONAL

El estado actual de conectividad, acceso, uso y adopción de las TIC en Paraguay muestra un avance significativo, con esfuerzos concretos en la consolidación de la infraestructura digital, lo que permite una mayor inclusión digital en zonas urbanas y rurales. El país ha fortalecido su red de banda ancha móvil, facilitando el acceso a Internet en espacios públicos y en instituciones educativas y de salud. Asimismo, la digitalización de servicios públicos está mejorando la eficiencia y la transparencia gubernamental, promoviendo un entorno más competitivo y productivo.

Cuadro 1. Indicadores de cobertura móvil en Paraguay

Cobertura red móvil	Dic 2023	Metas 2024	Metas 2025
Localidades con cobertura de telefonía móvil	**8.137**	8.165	8.234
Población con cobertura de telefonía móvil	**99,82%**	99,9%	100%
Localidades con cobertura de red 3G	**8.011**	7.825	7.900
Población con cobertura de red 3G	**99,60%**	99,2%	99,3%
Localidades con cobertura de Banda Ancha Móvil BAM 4G/LTE	**7.201**	7.650	7.800
Población con cobertura de Banda Ancha Móvil BAM (4G/LTE)	**96,89%**	98,43%	99,2%
Localidades con cobertura de Banda Ancha Móvil BAM 5G	**0**	0	100
Población con cobertura de Banda Ancha Móvil BAM 5G	**0%**	0%	10%

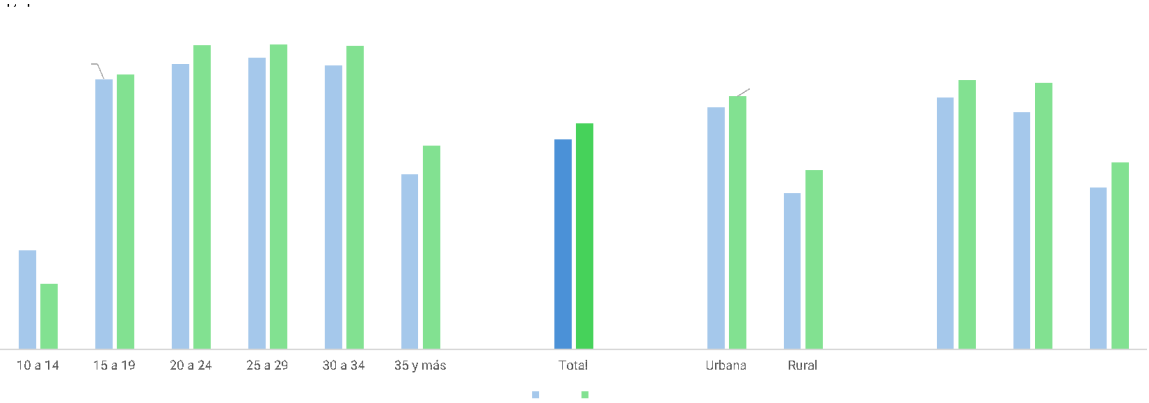
Fuente: Elaboración propia a partir de (CONATEL, 2024)

En Paraguay hay una notable mejora en el uso de Internet. En términos generales, el porcentaje de usuarios de Internet aumentó del 74.7% en 2022 al 78.1% en 2023. Se observa un incremento en las franjas etarias, con un crecimiento destacado en personas mayores de 30 años. En el área rural, el uso de Internet también mostró un incremento significativo, pasando del 63.2% al 68.2%, lo que indica un avance en la inclusión digital en

[6] A partir de los resultados del *Global Cybersecurity Index 2024 5th Edition* (ITU, 2024), el 80% de los países en la región Américas están en niveles "*T4. Evolving*" (51%) y en "*T3. Establishing*" (29%), incluido Paraguay en este último grupo.

zonas menos conectadas. Además, entre las personas ocupadas, el uso de Internet creció del 83.5% al 87.3%, mientras que en los desocupados aumentó del 80.4% al 86.7%, lo que refleja una mayor penetración de la conectividad en diferentes segmentos de la población.

Gráfica 1. Población de 10 y más años que utilizó Internet en Paraguay para 2022 y 2023 según grupos de edad, área de residencia y condición en la fuerza laboral



Nota: Los resultados según condición en la fuerza laboral se presentan para población de 15 y más años
Fuente: Elaboración propia a partir de INE. Encuesta Permanente de Hogares Continua 2017-2023.

Estos avances resaltan la importancia de promover el acceso equitativo a la tecnología y la mejora de la infraestructura, así como la necesidad de fortalecer la ciberseguridad para proteger a un número cada vez mayor de usuarios conectados. Un entorno digital seguro es esencial para consolidar la confianza ciudadana y empresarial, y para promover un ecosistema TIC robusto y sostenible en Paraguay.

2.1. Marco Normativo

En los últimos años, Paraguay ha logrado importantes avances en la consolidación de un marco normativo en materia de ciberseguridad. Estas acciones han sido impulsadas por la necesidad de fortalecer la infraestructura tecnológica y garantizar un entorno digital seguro para todos los sectores de la sociedad, ante el creciente número de amenazas cibernéticas.

A través de la celebración de acuerdos internacionales[7] y la promulgación de leyes, decretos, resoluciones, regulaciones, directrices y normativas específicas, Paraguay ha establecido unas bases para prevenir y gestionar riesgos de ciberseguridad y dar respuesta ante incidentes de ciberseguridad, promoviendo la cooperación internacional y la cooperación nacional entre el sector público, el sector privado y la ciudadanía en general. Estos esfuerzos buscan no solo proteger la infraestructura crítica y la información sensible, sino también fomentar la confianza en el entorno digital, un elemento clave para el desarrollo económico y social del país.

[7] El Cuadro 8 en el Anexo 1 de la Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay presenta los principales acuerdos internacionales relacionados con la ciberseguridad.

A nivel nacional, algunos fundamentos constitucionales en torno a la ciberseguridad se encuentran en la *Constitución Nacional* en: i) el artículo 2 donde se establece que en Paraguay la soberanía reside en el pueblo, ii) el Capítulo II del Título II de la Parte I que trata sobre los derechos de la libertad, en particular el artículo 9 que reconoce que toda persona tiene el derecho a ser protegida en su libertad y en su seguridad; el artículo 25 que reconoce que toda persona tiene el derecho a la libre expresión de su personalidad, a la creatividad y a la formación de su propia identidad; el artículo 26 que garantiza la libre expresión y la libertad de prensa, así como la difusión del pensamiento y de la opinión, sin censura alguna, y establece que toda persona tiene derecho a generar, procesar o difundir información; el artículo 30 que reconoce que la emisión y la propagación de las señales de comunicación electromagnética son del dominio público del Estado; el artículo 33 que reconoce que la intimidad personal y familiar, así como el respeto a la vida privada son inviolables, iii) el Capitulo III del Título II de la Parte I que trata sobre los derechos de la igualdad, en particular los artículos 46 de la igualdad de las personas, 47 de las garantías de la igualdad y 48 de la igualdad de derechos del hombre y de la mujer, y iv) el Capítulo II del Título I de la Parte II en la que la República del Paraguay, en sus relaciones internacionales, acepta el derecho internacional y se ajusta a los principios como la solidaridad y la cooperación internacional.

Por otra parte, el marco normativo relacionado con la ciberseguridad en Paraguay se compone de diversas leyes y decretos que abarca diversos temas que son fundamentales para el desarrollo de un entorno digital seguro y regulado[8]. Se destaca la normatividad en torno a: i) Privacidad, libertad de expresión y derechos humanos, i) Delito cibernético (sustantiva y procesal), iii) Comercio electrónico / Firma electrónica / Transacciones electrónicas / Expediente electrónico, iv) Protección al Consumidor, v) Tecnologías de la Información y las Comunicaciones, v) Protección Infantil en Línea, y vii) Propiedad Intelectual vii) Autoridad en ciberseguridad.

Adicionalmente, existen normas jurídicas y reglas dispersas en varios actos administrativos que regulan aspectos esenciales de la protección a la privacidad y de algunos datos personales, como los datos personales de naturaleza crediticia, sin embargo, no existe un marco normativo integral de protección de datos en Paraguay. Si bien, existen iniciativas y un borrador del marco en estudio, el mismo no está formalizado. De igual manera, se resalta la falta de legislación sobre información clasificada.

En relación con la normatividad sustantiva y procesal frente al delito cibernético, la Ley Nº 4439/2011[9] define las distintas conductas delictivas en las que interviene de alguna manera una actividad relacionada con las nuevas tecnologías de la información y las

[8] El Cuadro 9 en el Anexo 1 de la Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay presenta el marco constitucional, legal y regulatorio relacionado con la ciberseguridad.

[9] La Ley Nº 4439/2011 modificó tres (3) hechos punibles del *Código Penal*: i) Pornografía relativa a niños y adolescentes (Art. 140), ii) Sabotaje de sistemas informáticos (Art. 175) y iii) Estafa mediante sistemas informáticos (Art. 188); e introdujo nuevos hechos punibles al *Código Penal*: iv) Acceso indebido a datos (Art. 146b), v) Interceptación de datos (Art. 146c), vi) Preparación de acceso indebido e interceptación de datos (Art. 146d), vii) Acceso indebido a sistemas informáticos (Art. 174b), viii) Sabotaje de sistemas informáticos (Art. 175), , y ix) Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago (Art. 248b).

comunicaciones, no obstante, no se contempla expresamente el concepto de ciberdelito ni delito informático. Se centra en la protección mediante el derecho penal de datos y sistemas informáticos, excluyendo a los delitos cibernéticos en general.

En relación con la lucha contra el ciberdelito, una vez promulgada la Ley Nº 5994/2017 que aprueba su adhesión, Paraguay depositó el documento de adhesión el 30 de julio de 2018 el acceso al *Convenio sobre Ciberdelincuencia (Convenio de Budapest)* y al *Protocolo Adicional al Convenio sobre Ciberdelincuencia Relativo a la Penalización de Actos de índole Racista y Xenófoba cometidos por medio de Sistemas Informáticos*, los cuales entraron en vigor desde el 1 de noviembre de 2018. Además, el 24 de septiembre de 2024, Paraguay firmó el *Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia (Convenio de Budapest)* destinado a mejorar la cooperación y la divulgación de pruebas electrónicas.

En el marco de sus competencias[10], el MITIC ha establecido un marco normativo relacionado con la ciberseguridad[11] se destacan las diversas normativas aprobadas por Resolución de la entidad rectora dirigido a Organismos y Entidades del Estado (OEE) como la Resolución MITIC Nº 733/2019, que establece un modelo de gobernanza de seguridad de la información en el Estado, que tiene como objetivo la creación de un área de Seguridad de la Información en todas las instituciones gubernamentales, con objetivos, roles, competencias y responsabilidades bien definidas; la Resolución MITIC Nº 346/2020, que establece el reglamento de reporte obligatorios de incidentes cibernéticos de seguridad por parte los OEE, buscando centralizar la coordinación y respuesta ante incidentes cibernéticos.

Así mismo, la Resolución MITIC Nº 277/2020, que establece el estándar adoptado por el Gobierno, la Guía de Controles Críticos de Ciberseguridad (CIS Controls) con estándares mínimos de protección para los sistemas de información del Estado, asegurando que las organizaciones mejoren sus niveles de madurez en ciberseguridad implementando medidas de seguridad eficaces; la Resolución MITIC Nº 432/2019 que aprueba las Directivas de Ciberseguridad para Canales de Comunicación de medios oficiales del Estado, lo que es crucial para evitar la usurpación de identidad y la difusión de información no autorizada desde entidades gubernamentales.

Paraguay cuenta con un marco normativo importante en materia de ciberseguridad, no obstante, es necesario que se adecúe, adapte y/o armonice el marco normativo nacional en torno a la dinámica de la economía digital y sus incertidumbres inherentes, ya que es

[10] Ley 6207/2018, Artículo 7° Competencias inc. 5. Propiciar y emitir directrices para la optimización de los trámites y procesos, y la interoperabilidad entre los distintos Organismos y Entidades del Estado (OEE), a su vez diseñar, coordinar, y monitorear las políticas públicas, planes y estrategias a ser ejecutadas por los mismos, en el marco del Gobierno Electrónico y de Ciberseguridad.
Inc. 13- Dictar, asesorar y participar en la formulación de las políticas nacionales en todas aquellas materias relacionadas con la protección de la información personal y gubernamental; el uso de tecnologías en la educación, en materia de ciberseguridad.

[11] El Cuadro 10 en el Anexo 1 de la Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay presenta el marco técnico relacionado con la ciberseguridad.

complejo, disperso y desactualizado en muchos ámbitos relacionados con la ciberseguridad.

2.2. Plan Nacional de Ciberseguridad 2017

En relación con los temas específicos de ciberseguridad, Paraguay aprobó el Plan Nacional de Ciberseguridad 2017[12], producto de un trabajo de múltiples partes interesadas y de un proceso que involucró representantes de instituciones públicas, sector privado, academia, sociedad civil, organismos internacionales, entre otros.

Este Plan identificó, entre otras cosas, la necesidad de fortalecer los roles y atribuciones referentes a ciberseguridad y protección de la información, no sólo en cuanto a capacidad de respuesta a incidentes, sino también en cuanto a formación y concienciación, protección de infraestructuras críticas, seguridad en la administración pública, capacidad de investigación y persecución de la ciberdelincuencia y coordinación nacional[13]. Este Plan estableció ejes e iniciativas en varios ámbitos:

- *Sensibilización y Cultura*: una cultura nacional de ciberseguridad fortalecida, con un alto nivel de conciencia y conocimientos sobre prácticas seguras en el uso de tecnologías digitales. La ciudadanía, desde estudiantes hasta tomadores de decisiones, estaría mejor informada y preparada para enfrentar y reportar amenazas cibernéticas. Se lograría una sociedad más proactiva en la protección de sus datos y la prevención de delitos cibernéticos, lo que se traduciría en una mayor resiliencia frente a las amenazas digitales.

- *Investigación, Desarrollo e Innovación*: una integración de ciberseguridad en los programas educativos y el fomento de la investigación y el desarrollo en esta área estimularía el crecimiento de un ecosistema robusto de talento y capacidades técnicas. Esto impulsa la innovación en productos y servicios de ciberseguridad, fortaleciendo el sector TIC y fomentando una economía digital más segura y confiable. Además, se promovería la adopción de buenas prácticas y estándares de ciberseguridad en diversos sectores, fortaleciendo la confianza en el uso de las TIC.

- *Protección de Infraestructuras Críticas*: unas medidas normativas y técnicas para proteger las infraestructuras críticas. Se lograría una mejora en la capacidad de respuesta ante emergencias a través de simulacros y ejercicios regulares, y se fortalecería la cooperación internacional en esta área. Con una base de datos centralizada y directrices específicas, las organizaciones encargadas de gestionar infraestructuras críticas estarían mejor preparadas para identificar y mitigar riesgos cibernéticos.

[12] El Plan Nacional de Ciberseguridad 2017 cuenta con 20 objetivos estratégicos misionales y 60 líneas de acción operativas.
[13] El Anexo 2 de la Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay presenta los productos esperados de la implementación del Plan Nacional de Ciberseguridad 2017.

- *Capacidad de Respuesta ante Incidentes Cibernéticos*: unos mecanismos eficientes para la detección, respuesta y recuperación ante incidentes cibernéticos asegurando una capacidad nacional más sólida en la gestión de crisis digitales. Con una infraestructura actualizada y equipos capacitados, se mejoraría las capacidades del equipo de respuesta a incidentes nacional y colaborar efectivamente con otros actores, tanto a nivel nacional como internacional. Esto contribuiría a una respuesta más rápida y efectiva ante amenazas emergentes.

- *Capacidad de Investigación y Persecución de la Ciberdelincuencia*: una capacidad de las fuerzas del orden y el sistema judicial en la persecución de delitos cibernéticos que permitiría una acción más eficiente y efectiva contra la ciberdelincuencia. La implementación de recursos técnicos y capacitaciones, así como la cooperación internacional en la materia, resultaría en una mejora sustancial en la investigación y judicialización de estos delitos, garantizando un entorno más seguro para los ciudadanos y empresas.

- *Administración Pública y Coordinación Nacional*: un Sistema Nacional de Ciberseguridad con normativas claras y grupos de trabajo especializados que facilita una mejor coordinación y gestión de la ciberseguridad a nivel nacional. Se establecerán canales de comunicación eficientes entre los diferentes actores, incluyendo el sector privado y organismos internacionales, promoviendo un entorno colaborativo y ágil en la identificación y mitigación de amenazas. La administración pública estaría mejor equipada para adoptar e implementar soluciones de ciberseguridad de manera coherente y efectiva.

2.3. Sistema Nacional de Ciberseguridad

Paraguay cuenta con un Sistema Nacional de Ciberseguridad compuesto por una Autoridad Nacional de Ciberseguridad y un Centro de Respuestas ante Incidentes Cibernéticos (CERT).

El *Ministerio de Tecnologías de la Información y Comunicación (MITIC)* es la autoridad nacional en materia de ciberseguridad, y prevención, gestión y control de incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional, según lo establecido en la Ley Nº 6207/2018, el Decreto Presidencial Nº 2274/2019 y la Resolución MITIC Nº 346/2020.

El *Centro de Respuestas ante Incidentes Cibernéticos (CERT) del Paraguay (CERT-PY)* es una Dirección dentro de la Dirección General de Ciberseguridad y Protección de la Información (DGCPI) del MITIC brinda servicios de ciberseguridad para prevenir, detectar, mitigar y responder a incidentes cibernéticos en el que estén involucrados redes, sistemas o infraestructuras del país, tales como: i) gestión de incidentes cibernéticos, ii) publicaciones de boletines y alertas de seguridad, y iii) formación de capacidades, concientización y asesorías en ciberseguridad. A los Organismos y Entidades del Estado, le presta servicios exclusivos, tales como: i) auditoria de vulnerabilidades de sistemas, ii) reportes proactivos de ciberseguridad, iii) diagnósticos del nivel de madurez en ciberseguridad, iv) asistencia técnica de seguridad y v) simulacro de ciberataques.

Cuadro 2. Evolución de la gestión de incidentes por parte del CERT-PY

	2020	2021	2022	2023	2024
Reportes recibidos	2.100	2.299	3.668	2.661	1856
Incidentes atendidos	1.358	1.535	2.083	1.510	1424
Investigaciones realizadas	6.595	6.615	6.290	5.186	5340
Días de respuesta	6	0,71	4,46	2.9	2.1

Nota: A partir de la información 2020 y 2022, los incidentes atendidos por el CERT-PY anualmente son en promedio i) 0.3% de criticidad alta, ii) un 8.8% de criticidad media y un iii) 90.9% de criticidad baja.
Fuente: CERT-PY

El alcance de la gestión de un incidente cibernético por su parte abarca: i) el análisis preliminar del incidente cibernético, ii) la notificación, coordinación y guía a los actores involucrados y responsables de los sistemas afectados para la toma de acciones pertinentes, iii) la propuesta de recomendaciones pertinentes para la corrección y prevención futura, y iv) dependiendo de la naturaleza del incidente, de la solicitud y/o cooperación de un actor involucrado en un incidente y los procedimientos establecidos, el CERT-PY colabora en la aplicación de acciones de contención inmediatas, así como también en la investigación y análisis del sistema comprometido.

Cuadro 3. Evolución del tipo de incidente atendido por parte del CERT-PY

	2020	2021	2022	2023	2024
Equipo / Sistema comprometido	755	767	717	700	651
Software Malicioso (Malware)	726	627	687	693	629
Correo no deseado malicioso (Spam/Scam)	531	620	1183	589	326
Phishing	136	184	209	270	274
Escaneo / Fuerza Bruta	35	66	84	15	65
Problemas de configuración / Equipo vulnerable	11	30	16	6	17
Acceso indebido a cuentas, sistemas o datos	6	3	15	5	27
Ransomware	7	4	7	5	2
Denegación de servicios (DoS/DDoS)	2	10	0	21	33

Fuente: CERT-PY

Los principales tipos de incidentes atendidos por el CERT-PY son el compromiso de sistemas y equipos, el software malicioso (malware), y el correo no deseado malicioso (spam/scam), los cuales presentan un alto nivel de criticidad en términos de su impacto potencial en la ciberseguridad del país.

Cualquier ciudadano, empresa, institución pública u organización extranjera en el país puede reportar un incidente cibernético que afecte a un sistema de información del ecosistema digital nacional, propio o de terceros. Los procedimientos de gestión de incidentes cibernéticos utilizados por los analistas del CERT-PY se encuentran alineados a

los estándares internacionales y han sido establecidos con el objetivo de optimizar los tiempos de respuesta y resolución de incidentes cibernéticos, de una manera oportuna y eficaz. El CERT-PY es miembro activo del CSIRT Américas Network (https://csirtamericas.org/) de la Organización de Estados Americanos (OEA)[14].

Cuadro 4. Evolución del tipo de incidente atendido por parte del CERT-PY

	2020	2021	2022	2023	2024
Gobierno	123	1128	105	925	340
Privado	753	17	702	143	639
Extranjero	469	34	1266	102	173
Ciudadano	20	3	22	4	34
Educativo	2	844	4	1488	5

Fuente: CERT-PY

Por otra parte, y con el fin de combatir los hechos punibles cometidos a través de la tecnología en Paraguay, fue creada la Unidad Especializada de Delitos Informáticos en el Ministerio Público[15]. Los delitos informáticos se consideran como todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas utilizando herramientas tecnológicas e informáticas. La Unidad investiga el acceso indebido a sistemas informáticos, sabotaje de sistemas informáticos; estafa mediante sistemas informáticos, falsificación de tarjetas de débito o crédito, entre otros.

Cuadro 5. Evolución de las denuncias de hechos punibles cometidos a través de la tecnología en Paraguay

Hecho punible	2021	2022	2023
Pornografía relativa a niños y adolescentes	2.796	1.861	-
Sabotaje de sistemas informáticos	13	13	-

[14] Según CSIRT Americas Network de la OEA, el 2024 revela vulnerabilidades críticas en diversos sectores, particularmente en dominios educativos y gubernamentales del país. La plataforma identificó 35 sitios comprometidos y 562 cuentas de correo sospechosas, lo que indica un riesgo elevado de filtración de información sensible. La exposición de 7.379 credenciales, con un alarmante 97.6% de contraseñas en texto plano, aumenta considerablemente la probabilidad de accesos no autorizados a sistemas críticos. Además, la detección de 11.630 vulnerabilidades, incluyendo 680 críticas, en servidores web, protocolos de escritorio remoto y aplicaciones de correo electrónico, subraya la urgente necesidad de fortalecer la infraestructura digital del país. De particular preocupación es la identificación de 10 dispositivos ICS/SCADA vulnerables, que podrían comprometer servicios esenciales como el suministro de agua, electricidad y transporte aéreo. Este escenario demanda una respuesta estratégica integral que priorice la protección de infraestructuras críticas, la educación en ciberseguridad y la implementación de medidas robustas de prevención y respuesta a incidentes cibernéticos (CSIRT Americas Network, 2024).

[15] Esta Unidad fue creada en 2010 por Resolución FGE Nº 3459/2010 y ampliada por Resolución FGE 4408/2011. También brinda apoyo técnico - jurídico a los agentes fiscales en la realización de diligencias, conforme a lo establecido en el artículo 228 del C.P.P.; el registro o decomiso de datos informáticos almacenados, de conformidad a lo dispuesto en los artículos 183, 192, 193 y 196 del C.P.P. Actualmente realizan charlas en instituciones educativas de todo el país en el marco del programa Fiscalía en la Escuela. Funcionarios de la Unidad brindan capacitaciones sobre el ciberbulling, sexting, pornografía infantil y grooming, es decir, sobre los peligros y amenazas existentes contra los menores en Internet. (https://ministeriopublico.gov.py/unidad-especializada-de-delitos-informaticos-).

Hecho punible	2021	2022	2023
Estafa mediante sistemas informáticos	323	725	2314
Acceso indebido a datos	252	422	-
Interceptación de datos	1	1	-
Preparación de acceso indebido e interceptación de datos	1	0	-
Acceso indebido a sistemas informáticos	992	422	906
Sabotaje de sistemas informáticos	13	13	-
Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago	106	37	-
	4.497	**3.494**	**3535**

Fuente: Ministerio Público.

2.4. Nivel de Madurez de Capacidades

El marco normativo establecido a la fecha; el accionar del Sistema Nacional de Ciberseguridad al gestionar incidentes cibernéticos y la implementación de acciones derivadas del Plan Nacional de Ciberseguridad 2017, han contribuido significativamente a avanzar en el nivel de madurez de las capacidades de ciberseguridad de Paraguay, según se observa bajo las diversas metodologías que se aplican en las mediciones internacionales.

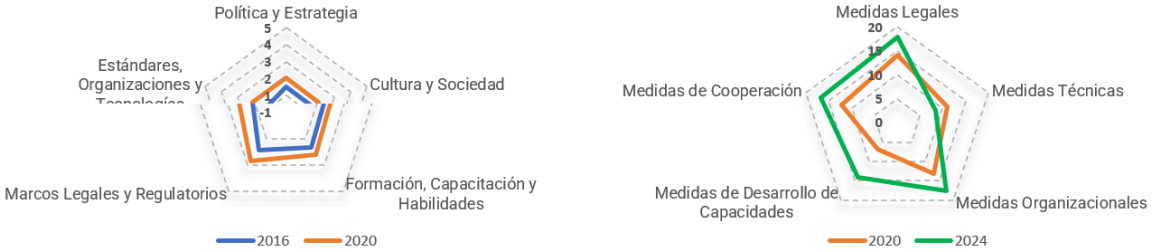
Según los resultados de la aplicación del *Modelo de Madurez de Capacidades de Seguridad Cibernética*[16] por parte de la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) se evidenció un avance integral entre 2016 y 2020 de todas las dimensiones que, en conjunto, constituyen la amplitud de la capacidad nacional que un país requiere para ser eficaz en la prestación de servicios de ciberseguridad. De manera similar y según las mediciones del *Global Cybersecurity Index (GCI*[17] de la Unión Internacional de Telecomunicaciones (UIT), se aprecia una evolución positiva entre 2020 y 2024 en aspectos relacionados con *Medidas Organizacionales* y con *Medidas de Desarrollo de Capacidades,* pero existen áreas con progresos limitados e incluso retrocesos, como es el caso de las *Medidas Técnicas*, donde se observa un decremento en el nivel de madurez.

Gráfica 2. Paraguay en mediciones internacionales de capacidades de ciberseguridad

Mediciones CMM de OEA & BID (2016 y 2020) **Mediciones GCI de UIT (2020 y 2024)**

[16] El Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM, por sus siglas en inglés, Cybersecurity Capacity Maturity Model for Nations) es un marco metódico diseñado por el Centro de Capacidad de Seguridad Cibernética Global del Departamento de Ciencias de la Computación de la Universidad de Oxford para revisar la capacidad de ciberseguridad de un país (GCSCC, 2024).

[17] El Global Cybersecurity Index (GCI) es un referente de confianza que mide el compromiso de los países con la ciberseguridad a nivel global (https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx).

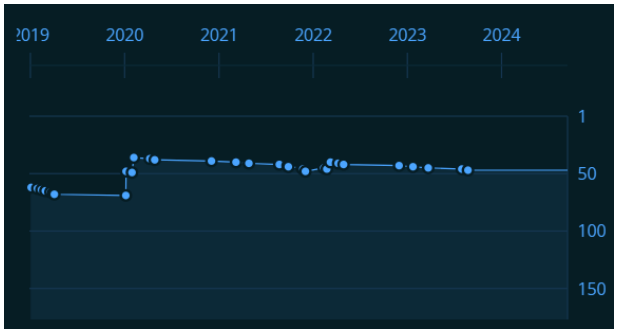


Fuente: Elaboración propia a partir de (OEA & BID, 2020), (ITU, 2023b) y (ITU, 2024)

De lo anterior, Paraguay presenta un progreso leve en la madurez de sus capacidades de protección, detección y respuesta ante incidentes. Esta situación debe revisarse, ya que el entorno digital continúa evolucionando rápidamente con la aparición de nuevas vulnerabilidades y vectores de ataque cada vez más sofisticados.

Para asegurar la resiliencia del país frente a estas amenazas emergentes, es imperativo que se fortalezcan las medidas de ciberseguridad a través de la actualización y mejora continua de las capacidades existentes, promoviendo un enfoque integral que contemple no solo las tecnologías y marcos regulatorios, sino también la cooperación internacional, la capacitación especializada y el desarrollo de una cultura de ciberseguridad robusta en todos los sectores de la sociedad.

Gráfica 3. Evolución de la medición del *National Cyber Security Index (NCSI)* del e-Governance Academy de Estonia para Paraguay



Fuente: (e-Governance Academy, 2024)

El contexto nacional actual sugiere la necesidad de redoblar esfuerzos en ciertos ámbitos específicos para abordar los respectivos retos y desafíos para alcanzar un desarrollo integral y sostenido en todas las dimensiones de la ciberseguridad.

2.5. Retos y desafíos

Desde el 2017, el camino recorrido por el país ha sido satisfactorio en varios aspectos, reflejando avances significativos en diversas áreas. Sin embargo, la implementación del plan de acción del Plan Nacional de Ciberseguridad 2017 fue compleja, especialmente en tiempos de la pandemia de COVID-19 y de la postpandemia en donde se generaron nuevos riesgos y desafíos. A esto se suma la persistente escasez de recursos de inversión, lo que

ha limitado el desarrollo óptimo de las iniciativas planteadas. A pesar de los avances logrados, existen retos y desafíos importantes que son necesarios abordar para garantizar un crecimiento sostenible y equitativo en el país, lo que demanda esfuerzos adicionales y un renovado compromiso.

Durante el año 2020, la *Comisión Nacional de Ciberseguridad* aprobó un mecanismo de medición cualitativo que permitiera medir el grado de cumplimiento de la ejecución de las diferentes acciones del Plan Nacional de Ciberseguridad 2017. A partir de los resultados de la evaluación, se aprecia un bajo nivel de implementación en la mayoría de sus ejes estratégicos. Los mayores avances se registraron en el eje de *Administración Pública y Coordinación Nacional* con un nivel de cumplimiento de 44%. Asimismo, la *Capacidad de Investigación y Persecución de la Ciberdelincuencia* logró un cumplimiento de 33%. Sin embargo, el avance en otros ejes fue limitado. Por ejemplo, en *Protección de Infraestructuras Críticas* se registró un cumplimiento muy bajo, con solo un 5% alcanzado, y el eje de *Investigación, Desarrollo e Innovación* registró solo un 17% de cumplimiento.

Cuadro 6. Nivel de cumplimiento en la implementación del Plan Nacional de Ciberseguridad 2017

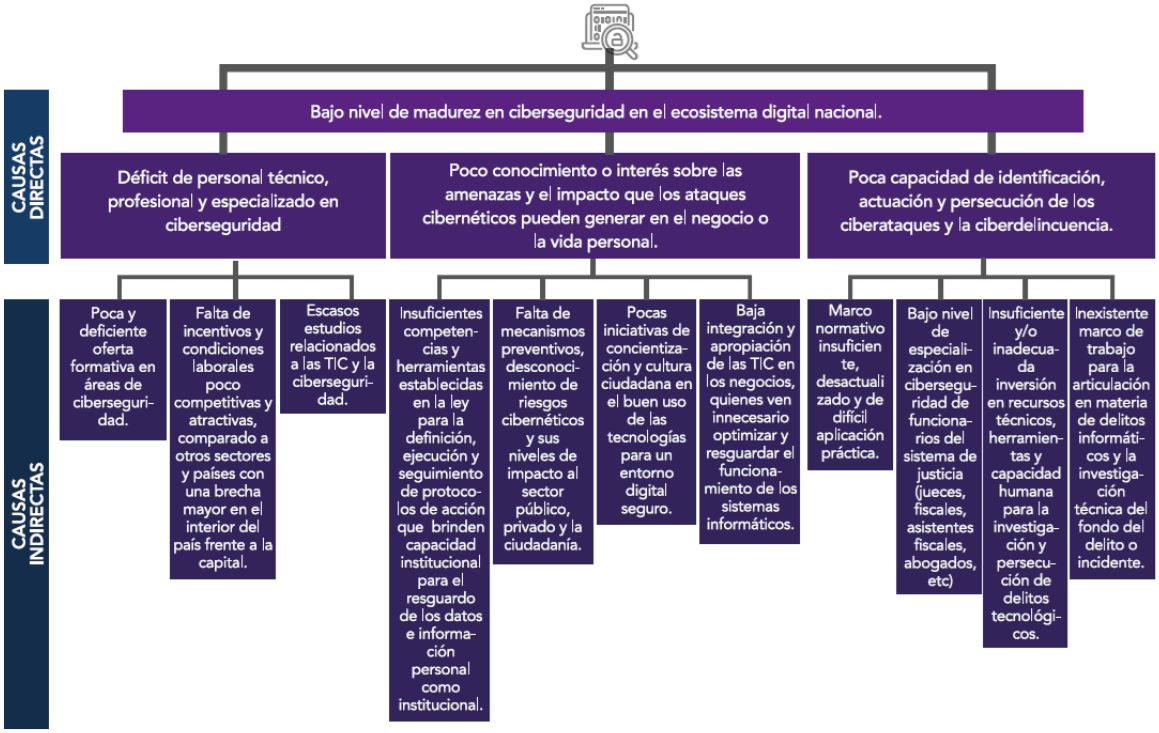
EJES	Nivel de cumplimiento	Mecanismo de Medición Cualitativo		
		Nivel 1	Nivel 2	Nivel 3
SENSIBILIZACIÓN Y CULTURA	**21%**	46%	46%	8%
INVESTIGACIÓN, DESARROLLO E INNOVACIÓN	**17%**	57%	36%	7%
PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS	**5%**	86%	14%	0%
CAPACIDAD DE RESPUESTA ANTE INCIDENTES CIBERNÉTICOS	**21%**	37%	63%	0%
CAPACIDAD DE INVESTIGACIÓN Y PERSECUCIÓN DE LA CIBERDELINCUENCIA	**33%**	22%	56%	22%
ADMINISTRACIÓN PÚBLICA Y COORDINACIÓN NACIONAL	**44%**	11%	45%	44%

Nota: Nivel 1 (No se realizó ninguna o prácticamente ninguna acción), Nivel 2 (se realizó alguna iniciativa o acción, pero de manera esporádica, no sistematizada ni sostenible) y Nivel 3 (la línea de acción se implementó de manera permanente y sostenible a través de alguna iniciativa aprobada por un instrumento legal (ley, decreto, resolución, etc.) y/o un programa con presupuesto fijo establecido)
Fuente: Elaboración propia a partir de (CERT-PY, 2020)

Durante el año 2022, el MITIC aprobó el *Plan Nacional TIC 2022-2030: Paraguay Equitativo, Transparente y Competitivo* con la hoja de ruta para el desarrollo y fortalecimiento del ecosistema TIC en Paraguay. En particular, esta política estableció cuatro (4) lineamientos estratégicos: i) Consolidación de la Infraestructura Digital, ii) Transformación Digital del Estado, iii) Fortalecimiento del Ecosistema TIC (Talento TIC e Innovación TIC) y iv) Fortalecimiento de la Ciberseguridad.

En relación con este último lineamiento estratégico, la PNTIC 2022-2030 identificó que existía en Paraguay un bajo nivel de madurez en ciberseguridad en el Ecosistema Digital nacional, generado por: i) déficit de personal técnico, profesional y especializado en ciberseguridad, ii) poco conocimiento o interés sobre las amenazas y el impacto que los ataques cibernéticos pueden generar en el negocio o la vida personal y iii) poca capacidad de identificación, actuación y persecución de los ciberataques y la ciberdelincuencia.

Gráfica 4. Causas de la problemática de ciberseguridad en Paraguay según el PNTIC 2022-2030



Fuente: (MITIC, 2022)

Durante el año 2024, la DGCPI y el CERT-PY del MITIC llevaron a cabo un proceso para la actualización y formulación de la Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay con el apoyo y acompañamiento de la Sección de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA). En el marco del proceso se adelantaron varias actividades bajo el enfoque de múltiples partes interesadas del ecosistema de ciberseguridad de Paraguay, así:

- Entre abril y mayo de 2024, se llevaron a cabo 12 mesas de trabajo virtuales con la participación de 100 representantes (76% hombres y 24% mujeres) de 30 entidades públicas y privadas recibiendo 130 observaciones al proceso. Estas sesiones contaron con la participación de entidades del Poder Ejecutivo, Legislativo y Judicial, además de asociaciones y referentes del sector de ciberseguridad.
- En mayo de 2024, se adelantó una reunión con 54 representantes de 32 OEE y otros actores del ecosistema de ciberseguridad.

- En junio de 2024, se lanzó el proceso de actualización y formulación de la Estrategia Nacional de Ciberseguridad 2025-2028 con una participación de 250 representantes de partes interesadas aportando insumos relevantes para el proceso de formulación.
- En julio de 2024, se adelantaron 3 mesas de trabajo presenciales con la participación de 110 representantes de las múltiples partes interesadas. Esta colaboración permitió adelantar una evaluación integral del estado actual de la ciberseguridad en Paraguay, identificar problemas y necesidades urgentes, sentando las bases para un sólido marco estratégico de la ciberseguridad.

A partir de las evaluaciones realizadas antes de 2024 y las diferentes actividades desarrolladas en el marco del proceso de actualización de la Estrategia Nacional de Ciberseguridad con las múltiples partes interesadas del ecosistema de ciberseguridad en Paraguay durante 2024, donde se ha solicitado explayarse en las principales problemáticas en ciberseguridad se identificaron los siguientes siete (7) retos de orden nacional:

- **Reto 1: Mejora continua en la coordinación de la gobernanza de ciberseguridad**. Paraguay enfrenta desafíos en su gobernanza de ciberseguridad debido a la falta de cadencia de una articulación estratégica que impide el desarrollo de políticas coherentes y efectivas. Además, hay cierta discontinuidad en la coordinación, cooperación, colaboración y comunicación entre las entidades gubernamentales, el sector privado y otras partes interesadas, lo que dificulta una respuesta unificada a las amenazas cibernéticas.

- **Reto 2: Recursos financieros limitados y asignación ineficiente en ciberseguridad.** Paraguay tiene limitaciones en sus fuentes de financiación para iniciativas de ciberseguridad, lo que resulta en una inversión y presupuesto insuficientes. La asignación eficiente de los recursos disponibles también es un desafío, ya que no siempre se destinan a las áreas más críticas, afectando la capacidad del país para fortalecer su infraestructura y respuesta cibernética.

- **Reto 3: Escasez de talento humano y falta de formación en ciberseguridad.** Existe una escasez de talento humano especializado y de habilidades en ciberseguridad en Paraguay. Las oportunidades de educación, capacitación y formación en este campo son limitadas, lo que conduce a una baja concientización sobre la importancia de la ciberseguridad en todos los niveles, desde usuarios individuales hasta profesionales y empresas.

- **Reto 4: Marco normativo desactualizado y carencia de definiciones claras.** Paraguay carece de un marco normativo integral y actualizado en materia de ciberseguridad. La falta de definiciones claras y un marco técnico sólido dificulta el cumplimiento de estándares internacionales y nacionales. Además, existe un vacío en el marco sancionatorio, lo que impide aplicar sanciones efectivas ante incumplimientos. La falta de legislación en relación con la protección de datos

personales también es insuficiente, exponiendo a los ciudadanos a riesgos de privacidad y seguridad.

- **Reto 5: Ausencia de estandarización en infraestructura y de adopción de tecnologías emergentes.** Paraguay enfrenta problemas críticos en la estandarización de su ciberseguridad debido a la falta de normas unificadas para su infraestructura tecnológica. La diversidad y obsolescencia en el hardware y software (HW/SW) utilizados por entidades públicas y privadas generan vulnerabilidades y dificultan la implementación de medidas de seguridad coherentes. La ausencia de plataformas y herramientas estandarizadas impide una gestión eficiente de riesgos y una respuesta coordinada ante incidentes cibernéticos. Además, el país no está incorporando adecuadamente las tecnologías emergentes, lo que limita su capacidad para modernizar sus sistemas y fortalecer su defensa contra amenazas cibernéticas avanzadas.

- **Reto 6: Insuficiente ciber resiliencia y protección de infraestructura crítica.** La protección de la infraestructura crítica en Paraguay es insuficiente debido a la falta de planes efectivos de gestión de crisis. No existen procedimientos establecidos para el reporte y divulgación de incidentes cibernéticos, ni un adecuado intercambio de información entre entidades. La ausencia de estandarización en infraestructura, tanto en hardware y software como en plataformas y herramientas, dificulta la implementación de medidas de seguridad consistentes. Además, el país no está aprovechando plenamente las tecnologías emergentes para fortalecer su ciber resiliencia.

- **Reto 7: Debilidades en la lucha contra el cibercrimen y gestión de evidencia digital.** El marco procesal y sustantivo vigente es insuficiente para abordar los delitos cibernéticos modernos. La falta de tipificación clara de estos delitos y la gestión inadecuada de la evidencia digital dificultan las investigaciones y enjuiciamientos. Además, hay una necesidad urgente de prevención, capacitación, formación y mayor concientización en este ámbito.

3. MARCO ESTRATÉGICO

La Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay está diseñada para abordar los retos y desafíos nacionales en torno a la ciberseguridad y para asegurar que los beneficios de la eliminación de las brechas en el acceso a las TIC, el acceso plural a todos los servicios del Estado, la transparencia en la gestión pública y la transformación digital de todos los sectores económicos se materialicen de manera segura, sostenible y resiliente.

A corto plazo, se enfoca en que Paraguay pueda aumentar la concienciación pública, y la aplicación de medidas de prevención, fortalecer las capacidades de respuesta a incidentes y construir asociaciones internacionales. A mediano plazo, aborda las brechas en los marcos legales y regulatorios, el combate al ciberdelito en forma integral, mejorar la cooperación público-privada y promover el desarrollo de habilidades en ciberseguridad. A

largo plazo, priorizar las inversiones sostenidas en infraestructura de ciberseguridad, investigación, desarrollo e innovación, y el desarrollo de la fuerza laboral para construir un futuro digital resiliente y seguro.

Todo esto se llevará a cabo por medio de un trabajo conjunto que incluye a todos los sectores, teniendo en cuenta la visión país de un Paraguay más equitativo, transparente y competitivo, bajo enfoques de inclusión, innovación y sostenibilidad. Además, se respetarán principios orientadores como la gobernanza, la transparencia y la gestión de riesgos. Al adoptar un enfoque holístico y coordinado, Paraguay podrá proteger a sus ciudadanos, empresas e instituciones de las amenazas cibernéticas, al tiempo que aprovecha todo el potencial de la era digital, impulsando un desarrollo económico y social sostenido.

3.1. Articulación estratégica

La Estrategia Nacional de Ciberseguridad 2025-2028 se construye a partir de lo dispuesto en los principales instrumentos de políticas nacionales junto con los planes y estrategias sectoriales e institucionales relacionadas. En específico, se destaca lo dispuesto en el *Plan Nacional TIC 2022-2030*[18] en donde la ciberseguridad es un habilitador del ecosistema TIC que debe ser fortalecido mediante cuatro líneas estratégicas clave:

i) Capacidad de Gestión de Incidentes Cibernéticos,
ii) Sistema de Intercambio de Información de Ciberseguridad,
iii) Protección de Sistemas de Gobierno e Infraestructura crítica, y
iv) Formación de Capacidades en Ciberseguridad y Concienciación.

Cuadro 7. Políticas, Planes y Estrategias nacionales relacionados con la Estrategia Nacional de Ciberseguridad 2024-2028

Tipo de instrumento	Instrumentos de política
Plan Nacional	Plan Nacional de Desarrollo Paraguay 2014-2030 [19]
	Plan Nacional TIC 2022-2030 [20]
	Plan Nacional de Ciberseguridad 2017
	Plan Nacional de Telecomunicaciones 2021-2025 [21]
	Plan Nacional de Educación 2024 [22]
	Plan Nacional de Pueblos Indígenas [23]
	Plan Nacional de Juventud
	IV Plan Nacional de Igualdad 2018-2024 [24]
Política Nacional	Política Nacional de la Niñez y la Adolescencia 2014-2024 [25]

[18] El Anexo 4 de la Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay presenta los lineamientos estratégicos, iniciativas y metas propuestas en el Plan Nacional TIC 2022 - 2030, actividades establecidas en el marco del Programa de Apoyo de la Agenda Digital para fortalecer la ciberseguridad.
[19] https://www.stp.gov.py/pnd/wp-content/uploads/2014/12/pnd2030.pdf
[20] https://drive.mitic.gov.py/index.php/s/xWyPqZQ99Jm8zYL
[21] https://www.conatel.gov.py/conatel/wp-content/uploads/2021/10/pnt_21-25_-_res._dir._2246-2021.pdf
[22] https://www.mec.gov.py/cms_v2/adjuntos/2344
[23] https://www.indi.gov.py/application/files/8716/1903/8084/Plan_Nacional_Pueblos_Indigenas_-_version_digital.pdf
[24] https://oig.cepal.org/sites/default/files/paraguay_2018-2024_plan_de_igualdad.pdf
[25] https://informacionpublica.paraguay.gov.py/public/3852576-PolticaNacionaldeNiezyAdolescencia-POLNA.pdf

	Política Nacional de Defensa 2019-2030 [26]
	Política Militar de Defensa 2019 – 2030
	Política Nacional de Ciberdefensa [27]
Plan Estratégico	Plan Estratégico para la Seguridad para el Desarrollo 2023-2028 [28]
Estrategia Nacional	Estrategia de Transformación Digital – Agenda Digital [29]
	Estrategia Nacional de Innovación [30]
	Estrategia de Estadísticas de Género Paraguay 2021-2025 [31]
	Directiva de Defensa Nacional

Fuente: Elaboración propia

Cada uno de los instrumentos de política identificados integra iniciativas y esfuerzos de política pública que el país está planteando para los próximos años y que tienen relación directa o indirecta con la ciberseguridad. Por lo tanto, la Estrategia Nacional de Ciberseguridad 2025-2028 aborda no solo las iniciativas que estará implementando el MITIC, como ente rector del sector de las TIC y como autoridad nacional de ciberseguridad, sino también aquellas que estarán desarrollando los otros OEE para impulsar la madurez de capacidades nacionales de ciberseguridad. Lo anterior, entendiendo que la ciberseguridad es una apuesta a nivel país que involucra y requiere los esfuerzos de todas las múltiples partes interesadas en conjunto con el sector público.

Esta estrategia también se articula con políticas específicas de ciberseguridad relacionadas con la defensa nacional y la seguridad pública. En el ámbito de la defensa nacional, liderado por el Ministerio de Defensa Nacional (MDN) y las Fuerzas Armadas, se fortalecerán las capacidades de ciberdefensa mediante la integración de unidades especializadas en el ámbito militar, el establecimiento de protocolos conjuntos para la protección de infraestructuras críticas y la coordinación con organismos internacionales para la adopción de mejores prácticas.

Asimismo, en el ámbito de la seguridad pública, encabezado por el Ministerio del Interior y la Policía Nacional, se implementarán medidas para prevenir y combatir el ciberdelito a través del fortalecimiento de las unidades de cibercrimen y la formación de sus agentes en nuevas tecnologías, trabajando en conjunto con la Fiscalía para garantizar una investigación y persecución efectiva de los delitos cibernéticos. Estas acciones se articularán con los esfuerzos globales de Paraguay en ciberseguridad, asegurando un enfoque integral que contemple la protección de sus infraestructuras estratégicas, la seguridad ciudadana y la defensa de su soberanía digital.

3.2. Enfoques rectores

La Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay se formula para ser implementada bajo los siguientes enfoques estratégicos nacionales:

[26] https://mdn.gov.py/wp-content/uploads/2023/09/Politica_de_Defensa_Nacional_2019-2030.pdf
[27] https://digetic.mil.py/wp-content/uploads/2023/06/Resolocuion-No-573-refernte-a-Politica-de-Ciberdefensa-2.pdf
[28] https://www.antsv.gov.py/application/files/9617/2979/4676/CODENA_PARAGUAY__Plan_Seguridad_para_el_Desarrollo_2023_-_2028__VERSION_COMPLETA_1.pdf
[29] https://mitic.gov.py/agendadigital/
[30] https://innovacion.gov.py/
[31] https://www.sfp.gov.py/vchgo/application/files/2817/0845/3391/Visualizar.pdf

- **Centrado en el ser humano**: promueve la participación de Toda la Sociedad en el diseño y evaluación de políticas de ciberseguridad, involucrando a las múltiples partes interesadas y priorizando el acceso equitativo a herramientas y formación, especialmente para grupos vulnerables, asegurando que todos, sin importar su situación socioeconómica, ubicación o género, puedan desarrollar habilidades para enfrentar los desafíos digitales. Además, se abordarán los riesgos e impactos diferenciados de las amenazas cibernéticas, de modo que la ciberseguridad responda a las necesidades complejas e interseccionales de las personas en Paraguay, considerando factores como el género, la orientación sexual, la edad, la raza, la religión, la etnia, la capacidad, el nivel socioeconómico, la nacionalidad, la ruralidad y la afiliación política, entre otros.

- **Innovación**: se fundamenta en la innovación, promoviendo el desarrollo y la adopción de tecnologías emergentes y avanzadas que fortalezcan la capacidad de respuesta y defensa ante amenazas cibernéticas. Además, acompaña la creación de marcos regulatorios flexibles y adaptativos que permitan la implementación de nuevas tecnologías sin comprometer la seguridad. La colaboración con el sector privado y la comunidad internacional es clave para mantenerse a la vanguardia en la protección de infraestructuras críticas y la prevención de ciberataques.

- **Sostenibilidad**: asegura que las iniciativas implementadas tengan un impacto duradero y que puedan adaptarse a largo plazo frente a la evolución constante de las amenazas cibernéticas. Esto implica desarrollar capacidades locales a través de la formación continua de talento en ciberseguridad, la creación de mecanismos de financiamiento sostenible para proyectos de ciberseguridad y el establecimiento de políticas y normas que fomenten una cultura de seguridad cibernética a nivel nacional. Además, la sostenibilidad requiere una visión estratégica que priorice la resiliencia del ecosistema digital del país, minimizando la dependencia de recursos externos y fortaleciendo la autonomía tecnológica de Paraguay.

3.3. Visión

Para 2028, Paraguay será un país donde la ciberseguridad constituya una prioridad nacional para todos los actores, desde el gobierno hasta la ciudadanía. Se habrá consolidado un ecosistema digital seguro, sostenible y resiliente, respaldado por una fuerza laboral especializada y un marco normativo claro que permita enfrentar de manera efectiva las ciberamenazas y el cibercrimen.

3.4. Principios orientadores

La Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay aplica los siguientes principios orientadores:

- **Gobernanza**: Garantizar una gobernanza efectiva estableciendo un marco claro de políticas, roles y responsabilidades que facilite la coordinación y la toma de decisiones entre todas las partes involucradas en la ciberseguridad.

- **Gestión de riesgos**: Adoptar una gestión proactiva de riesgos evaluando continuamente las amenazas cibernéticas, identificando, priorizando y aplicando medidas adecuadas para minimizar vulnerabilidades, protegiendo así las infraestructuras críticas y los sistemas de información.

- **Cooperación y Colaboración**: Abordar la ciberseguridad de manera integral fomentando la cooperación y colaboración interinstitucional entre el sector público, el sector privado, la academia, la sociedad civil, y la comunidad internacional, compartiendo información y recursos para fortalecer colectivamente la ciberseguridad y combatir amenazas transfronterizas.

- **Prevención**: Priorizar la prevención mediante la implementación de medidas proactivas contra ciberataques, garantizando la continuidad de los servicios esenciales, como la educación y concienciación en ciberseguridad en todos los niveles educativos, la formación, capacitación y el desarrollo de habilidades y capacidades técnicas para evitar la ocurrencia de incidentes cibernéticos.

- **Respuesta y Resiliencia:** Proteger los activos digitales, dando respuestas efectivas de contención, erradicación, recuperación e investigación ante incidentes cibernéticos y desarrollar una mayor resiliencia para prevenir ataques cibernéticos y acelerar la recuperación.

- **Responsabilidad compartida**: Reconocer que la ciberseguridad es una responsabilidad compartida donde cada actor, desde individuos hasta organizaciones de todos los sectores, debe estar involucrado conociendo los riesgos y amenazas y contribuyendo activamente a la protección del ecosistema digital nacional.

- **Confianza y Transparencia**: Actuar con transparencia y fomentar una cultura de colaboración en el ciberespacio, comunicando abiertamente políticas y medidas tomadas en materia de ciberseguridad, para construir confianza pública entre las organizaciones y ciudadanos, permitiendo compartir información sobre amenazas, vulnerabilidades y mejores prácticas, fortaleciendo así la comunidad de ciberseguridad, aprendiendo de los errores de los demás, y ayudando a una respuesta más eficaz a las amenazas para detectar y responder a amenazas similares de manera más rápida.

- **Adaptabilidad, Flexibilidad y Sostenibilidad**: Evolucionar junto con el entorno digital dinámico para adaptarse rápidamente a las nuevas amenazas, técnicas de ataques y desafíos que surgen en el ciberespacio, como la rápida adopción de nuevas tecnologías, sin comprometer la seguridad siendo sostenibles a largo plazo.

3.5. Objetivo general

Fortalecer la ciberseguridad nacional de Paraguay mediante una estrategia integral que garantice la protección de los servicios digitales, el desarrollo de un entorno seguro y la resiliencia ante ciberamenazas. Para ello, se establecerán marcos normativos claros, se promoverá la formación de profesionales en la materia y se fomentará la cooperación interinstitucional. Asimismo, se impulsará una inversión eficiente en infraestructura y tecnología, asegurando la protección de infraestructuras críticas y el fortalecimiento de la capacidad de respuesta ante incidentes cibernéticos.

3.6. Dimensiones, Líneas Estratégicas y Objetivos Específicos

Bajo la implementación de todas las acciones y el cumplimento de los objetivos específicos construiremos, de manera integrada y coordinada de todas las partes interesadas, y junto a la ciudadanía un Paraguay ciberseguro: invirtiendo en nuestro futuro digital, desarrollando una fuerza laboral especializada en ciberseguridad, estableciendo y cumpliendo reglas claras en el ciberespacio, promoviendo el uso de un lenguaje técnico común, estando preparados y ciber resilientes, y unidos contra el cibercrimen y amenazas cibernéticas como el ransomware.

3.6.1. Construir juntos un Paraguay ciberseguro

Fortalecer el liderazgo y fomentar una coordinación efectiva y sinérgica en ciberseguridad para proteger a la ciudadanía de las amenazas cibernéticas y garantizar una gestión unificada y proactiva de los riesgos en todo el país.

3.6.1.1. Consolidar una gobernanza nacional fuerte y cohesionada en ciberseguridad

3.6.1.1.1. Realizar una evaluación exhaustiva del modelo de gobernanza del Sistema Nacional de Ciberseguridad y, con base en los resultados, proponer e implementar las modificaciones necesarias para adaptar el sistema al nuevo contexto nacional e internacional de ciberseguridad.

3.6.1.1.2. Desarrollar un plan de implementación del modelo de gobernanza del Sistema Nacional de Ciberseguridad liderado por el Ministerio de Tecnologías de la Información y Comunicación (MITIC) por medio de la Dirección General de Ciberseguridad y Protección a la Información, el Coordinador Nacional de Ciberseguridad y el CERT-PY que incluya cronogramas y responsabilidades claras para todas las instancias del modelo de gobernanza nacional, incluyendo indicadores de desempeño que aseguren su correcta ejecución y revisión periódica.

3.6.1.1.3. Diseñar y lanzar una plataforma digital de participación ciudadana y colaboración interinstitucional en ciberseguridad, que permita el diálogo constante entre el sector público, sector privado, la academia, la sociedad civil y la comunidad internacional incluyendo módulos para la recepción de

reportes, la difusión de información y un foro para el intercambio de ideas y soluciones.

3.6.1.1.4. Desarrollar y ejecutar un plan integral de fortalecimiento institucional para la autoridad nacional de ciberseguridad, incluyendo la capacitación especializada de su personal, la mejora de su infraestructura tecnológica y la creación de un equipo especializado en la coordinación de políticas de ciberseguridad a nivel nacional.

3.6.1.1.5. Crear e implementar canales de comunicación seguros y efectivos entre las partes interesadas en ciberseguridad, tales como una red nacional de intercambio de información y un boletín periódico con actualizaciones sobre las mejores prácticas y amenazas emergentes. Estos canales deben estar basados en estándares internacionales de seguridad de la información.

3.6.1.1.6. Lanzar campañas nacionales e integrales de concienciación en ciberseguridad, dirigidas a diversos públicos objetivos, tales como niños, jóvenes, empresas, profesionales y ciudadanos en general. Estas campañas incluirán la creación de materiales multimedia interactivos, como videos educativos, infografías y guías prácticas, que se difundirán a través de plataformas digitales, redes sociales y medios de comunicación tradicionales.

3.6.1.1.7. Desarrollar y poner en marcha un sistema de reportes periódicos para informar a los sectores interesados y la ciudadanía en general sobre el progreso y la efectividad en la implementación de la Estrategia Nacional de Ciberseguridad 2025-2028, utilizando múltiples canales de comunicación. Incluyendo la publicación de informes anuales accesibles al público en un portal web interactivo dedicado, la realización de boletines periódicos que detallen los avances clave, y la organización de foros públicos y campañas de sensibilización para fomentar la participación ciudadana. Adicionalmente, se contempla un sistema de indicadores medibles que permita evaluar el impacto real de la estrategia y ajustar las acciones según los resultados obtenidos.

3.6.1.2. Impulsar una cooperación internacional dinámica y efectiva en ciberseguridad

3.6.1.2.1. Incorporar la ciberseguridad como un pilar central de la Política Exterior y en la agenda diplomática e internacional del país, desarrollando una estrategia específica para abordar asuntos de ciberseguridad en negociaciones bilaterales y multilaterales, así como en tratados internacionales.

3.6.1.2.2. Contribuir activamente en foros internacionales clave sobre ciberseguridad mediante la presentación de propuestas nacionales concretas y la participación en grupos de trabajo que diseñen soluciones colaborativas para desafíos globales.

3.6.1.2.3. Establecer acuerdos bilaterales de cooperación en ciberseguridad con países estratégicos, implementando marcos operativos conjuntos para la respuesta a incidentes y el intercambio de inteligencia sobre amenazas.

3.6.1.2.4. Definir y promover una postura nacional sólida sobre la aplicación de normas y principios de conducta responsable en el ciberespacio, articulando la posición en reuniones diplomáticas y creando guías para la implementación de marcos legales internacionales en el ámbito nacional.

3.6.1.2.5. Continuar los esfuerzos para impulsar las medidas de fomento de la confianza en el ciberespacio, desarrollando una estrategia específica para implementar las acciones correspondientes a nivel nacional.

3.6.2. Invertir en nuestro futuro digital

Asegurar una inversión adecuada y el uso eficiente de los recursos de inversión en ciberseguridad, de modo que se fortalezca las capacidades nacionales de ciberseguridad y se beneficie toda la Sociedad.

3.6.2.1. Asignar de manera eficiente los recursos actuales de ciberseguridad

3.6.2.1.1. Realizar una evaluación de la inversión pública en ciberseguridad en los Organismos y Entidades del Estado (OEE) para identificar y mapear los recursos destinados a ciberseguridad en el sector público, y generar recomendaciones a las autoridades para una asignación más eficiente y estratégica de dichos recursos.

3.6.2.1.2. Elaborar una Guía para la Formulación de Proyectos de Inversión Pública de Ciberseguridad para facilitar a los OEE la correcta planificación y ejecución de proyectos de ciberseguridad, mejorando así la capacidad del sector público para enfrentar amenazas y gestionar recursos de manera efectiva.

3.6.2.1.3. Elaborar una Guía para la Evaluación Socioeconómica de Proyectos de Inversión Pública de Ciberseguridad para dotar a los OEE de herramientas que permitan evaluar el retorno socioeconómico de los proyectos, mediante enfoques costo-beneficio o costo-eficiencia, justificando la inversión y optimizando el uso de los recursos públicos.

3.6.2.1.4. Capacitar a los funcionarios responsables de formular y evaluar Proyectos de Inversión Pública de Ciberseguridad para fortalecer las competencias técnicas y de gestión de los encargados de asegurar que los proyectos de ciberseguridad sean eficientes, viables y alineados con los objetivos de la Estrategia Nacional de Ciberseguridad.

3.6.2.1.5. Realizar auditorías periódicas en los OEE para garantizar la transparencia y la eficiencia en la asignación y uso de los recursos públicos destinados a ciberseguridad, identificando posibles áreas de mejora y asegurando el cumplimiento de los objetivos de la Estrategia Nacional de Ciberseguridad.

3.6.2.2. Movilizar nuevos recursos para la ciberseguridad nacional

3.6.2.2.1. Diversificar las fuentes de financiación para fomentar la formulación, ejecución y evaluación de Proyectos de Inversión de Ciberseguridad, mediante la creación de un mecanismo formal de alianzas público-privadas y la implementación de estrategias de cooperación internacional con organismos multilaterales y agencias de cooperación. Se desarrollará una plataforma de coordinación que facilite la vinculación de inversionistas y donantes con proyectos estratégicos de ciberseguridad.

3.6.2.2.2. Diseñar y proponer un esquema de incentivos fiscales y financieros para empresas que inviertan en mejoras de ciberseguridad, enfocándose especialmente en Pequeñas y Medianas Empresas (PYMEs). Este esquema incluirá la propuesta de deducciones fiscales por inversiones en ciberseguridad, así como la creación de subvenciones y créditos preferenciales para aquellas empresas que adopten buenas prácticas y mejoren sus capacidades de ciberseguridad.

3.6.2.2.3. Capacitar a gestores y administradores en planificación y gestión financiera para ciberseguridad, a través de la creación de un programa nacional de formación en gestión financiera, con módulos específicos sobre evaluación de riesgos, inversión en tecnologías de ciberseguridad y gestión de proyectos estratégicos.

3.6.3. Desarrollar una fuerza laboral especializada en ciberseguridad

Promover la educación y formación especializada en ciberseguridad para contar con más profesionales con más habilidades que protejan nuestra información y sistemas, aumentando la madurez de capacidades de ciberseguridad del país.

3.6.3.1. Fortalecer la oferta del mercado laboral en ciberseguridad

3.6.3.1.1. Implementar programas educativos que fomenten la alfabetización digital en la población infantil y juvenil, integrando contenidos que promuevan vocaciones en Ciencia, Tecnología, Ingeniería y Matemáticas (STEM), a través de alianzas con el sector educativo para desarrollar currículos actualizados y actividades extracurriculares enfocadas en STEM.

3.6.3.1.2. Recopilar y difundir un compendio de buenas prácticas para promover la conciencia sobre la carrera de ciberseguridad entre niños y jóvenes, mediante la creación de una plataforma en línea que recoja casos de éxito, recursos educativos y testimonios de profesionales en el campo.

3.6.3.1.3. Lanzar campañas nacionales de sensibilización sobre privacidad y ciberseguridad, dirigidas a jóvenes usuarios de tecnología, mediante la realización de ejercicios masivos de capacitación tanto en entornos educativos como a través de redes sociales, complementados por el desarrollo de materiales interactivos que fortalezcan sus habilidades en seguridad digital.

3.6.3.1.4. Desarrollar una plataforma tecnológica para identificar y atraer a estudiantes con alto potencial en ciberseguridad, utilizando herramientas de evaluación basadas en competencias y preferencias, facilitando su

acceso a programas de formación especializados y oportunidades de empleo en el sector.

3.6.3.1.5. Crear guías y recursos educativos que ayuden a los estudiantes y solicitantes de empleo a comprender las rutas de aprendizaje y certificaciones en ciberseguridad, mediante la publicación de un mapa interactivo que les permita tomar decisiones informadas sobre su formación y desarrollo profesional.

3.6.3.1.6. Impulsar la estandarización nacional de los currículos y planes de estudios en ciberseguridad que sirva de referencia para las instituciones educativas y permita definir de manera clara carreras profesionales en el campo de la ciberseguridad.

3.6.3.1.7. Organizar competencias y hackathons nacionales en ciberseguridad para incentivar el desarrollo de habilidades prácticas, en temas relacionados con la ciberseguridad, como por ejemplo la criptografía, promoviendo la participación de estudiantes, profesionales de otros sectores y entusiastas de la ciberseguridad. Estos eventos estarán respaldados por alianzas con instituciones académicas y el sector privado y se llevarán a cabo de manera regular, tanto a nivel nacional como regional.

3.6.3.2. Impulsar la demanda del mercado laboral en ciberseguridad

3.6.3.2.1. Desarrollar, en colaboración con la academia y la industria, un Marco Nacional de Competencias y Roles de Ciberseguridad, alineado con estándares internacionales como aquellos de la Organización Internacional de Normalización (ISO) y de la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) del Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST), que especifique las competencias, habilidades, y certificaciones necesarias para cada nivel profesional y practicante de ciberseguridad en el país. Este marco será publicado en una plataforma digital de acceso libre y actualizado periódicamente para asegurar su relevancia.

3.6.3.2.2. Crear e implementar un Sistema Nacional de Acreditación de Profesionales y Practicantes de Ciberseguridad, que evalúe a los candidatos a través de exámenes estandarizados basados en el Marco Nacional de Competencias y Roles de Ciberseguridad, otorgue certificaciones oficiales y supervise la renovación continua de estas certificaciones mediante programas de formación continua. El sistema incluirá una plataforma en línea para la gestión de las acreditaciones y certificaciones.

3.6.3.2.3. Fortalecer las capacidades en los OEE para reclutar y contratar talento en ciberseguridad, a través de la creación de guías de contratación especializadas, la realización de talleres de formación en recursos humanos para ciberseguridad y el uso de plataformas digitales de reclutamiento que conecten a los OEE con profesionales acreditados en ciberseguridad.

3.6.3.2.4. Implementar mecanismos de incentivos para motivar a las organizaciones públicas y privadas a desarrollar y promover marcos de trayectoria

profesional en ciberseguridad, mediante la creación de programas de reconocimiento y certificación de buenas prácticas en la gestión del talento en ciberseguridad.

3.6.3.2.5. Desarrollar e implementar programas específicos para promover la diversidad en la fuerza laboral de ciberseguridad, con un enfoque en mejorar el equilibrio de género y aumentar la representación de grupos subrepresentados en todos los niveles. Estos programas incluirán la creación de becas, mentorías y redes de apoyo dirigidas a mujeres y otras minorías en el campo de ciberseguridad.

3.6.3.2.6. Diseñar y ejecutar un plan nacional para que los OEE identifiquen, atraigan y retengan el mejor talento en ciberseguridad, promoviendo iniciativas innovadoras de capacitación continua, programas de desarrollo profesional y esquemas de reconocimiento de competencias. Este plan también incluirá programas de incentivos para la retención de talento, como oportunidades de crecimiento profesional y acceso a programas de formación avanzada.

3.6.4. Establecer y cumplir reglas claras en el ciberespacio

Actualizar el marco legal y regulatorio relacionado con ciberseguridad para brindar una protección legal efectiva a la ciudadanía y a todas las múltiples partes interesadas en el entorno digital.

3.6.4.1. Impulsar la actualización y modernización del marco legal y regulatorio de ciberseguridad

3.6.4.1.1. Adoptar un estándar oficial de términos y conceptos clave en ciberseguridad dentro del marco legal nacional, mediante la creación de una mesa de trabajo conformada por expertos en ciberseguridad, derecho y normativas internacionales. Esta mesa de trabajo tendrá la tarea de definir y validar un documento normativo que defina claramente los conceptos y términos fundamentales de ciberseguridad asegurando su coherencia con otros estándares internacionales.

3.6.4.1.2. Impulsar el desarrollo y aprobación de una Ley Marco de Ciberseguridad y Protección de Infraestructuras de Información Críticas Nacionales (IICN), estableciendo un grupo de trabajo multisectorial conformado por representantes del gobierno, la industria, la academia y la sociedad civil para elaborar un borrador legislativo que aborde las necesidades y desafíos del país en estas áreas. El proceso incluirá la realización de consultas públicas y mesas de diálogo con actores clave para asegurar que la ley sea inclusiva y refleje las mejores prácticas internacionales.

3.6.4.1.3. Llevar a cabo una estrategia de incidencia legislativa del borrador legislativo que incluirá presentaciones ante el Congreso y campañas de sensibilización pública para generar apoyo político y social. Además, se desarrollarán informes técnicos y análisis de impacto que evidencien la

importancia de la regulación para la protección del ciberespacio y de las infraestructuras críticas del país.

3.6.4.1.4. Impulsar la actualización y modernización del marco legal y regulatorio en materia de ciberseguridad, alineándose con estándares internacionales y mejores prácticas en temas como privacidad, libertad de expresión, derechos humanos, comercio electrónico, firma, expediente y transacciones electrónicas, protección al consumidor, protección de datos personales, tecnologías de la información y comunicación, protección infantil en línea, protección a la mujer y propiedad intelectual.

3.6.5. Promover el uso de un lenguaje técnico común

Implementar estándares comunes y adoptar nuevas tecnologías para mejorar la ciberseguridad y la eficiencia de nuestros sistemas digitales, facilitando una mejor protección de las Infraestructuras de Información Críticas Nacionales (IICN) en el país.

3.6.5.1. Establecer y adoptar estándares nacionales sólidos en ciberseguridad

3.6.5.1.1. Desarrollar un marco nacional de estandarización tecnológica que cubra infraestructura, hardware, software y plataformas, mediante la creación de mesa de trabajo técnica para la estandarización que coordine la elaboración de directrices y normas específicas para asegurar la homogeneidad tecnológica en todo el sector público y en sectores de IICN del país. Este marco será publicado como normativa oficial y actualizado periódicamente.

3.6.5.1.2. Promover la adopción de estándares y mejores prácticas internacionales en ciberseguridad y tecnología, facilitando su integración mediante campañas de concienciación y formación dirigidas a las entidades públicas y privadas, y estableciendo un portal digital donde se difundan los principales estándares internacionales globales y guías prácticas de implementación.

3.6.5.1.3. Establecer políticas nacionales de adquisición y actualización tecnológica, priorizando soluciones seguras y compatibles con el marco de estandarización, mediante la creación de un catálogo de tecnologías recomendadas y el diseño de criterios de evaluación obligatorios para todas las adquisiciones del sector público. Se promoverá que los principios de seguridad por diseño y por defecto se incluyan en los procesos de licitación de productos y servicios de tecnologías de la información y las comunicaciones por parte de los OEE. Este catálogo incluirá proveedores aprobados y tecnologías evaluadas según su seguridad y compatibilidad.

3.6.5.1.4. Implementar programas nacionales para la homologación de sistemas y herramientas, con el objetivo de facilitar la interoperabilidad entre plataformas utilizadas en infraestructuras críticas. Este programa incluirá un proceso de certificación de herramientas y tecnologías que cumplan con los requisitos de interoperabilidad y seguridad, apoyado por un centro de pruebas nacional para asegurar su efectividad.

3.6.5.1.5. Crear e implementar un Sistema de Certificación de Productos y Soluciones Tecnológicas de Ciberseguridad, estableciendo un proceso formal de evaluación y certificación que asegure que los productos y soluciones que se provean en el país cumplen con los estándares nacionales e internacionales de seguridad. Se crearán los criterios de evaluación, en colaboración con expertos del sector y alineado con normativas internacionales.

3.6.5.1.6. Fortalecer la seguridad de la cadena de suministro digital como eje estratégico de protección de las infraestructuras críticas nacionales. Implementar mecanismos de verificación, auditorías técnicas y esquemas de certificación obligatorios para todos los componentes tecnológicos que se integren a sistemas críticos, incluyendo hardware, software, firmware y servicios provistos por terceros. Reducir los riesgos asociados a proveedores nacionales e internacionales mediante el establecimiento de controles técnicos rigurosos que garanticen la integridad de los sistemas y eviten la introducción de componentes comprometidos o código malicioso.

3.6.5.2. Fomentar la investigación y el desarrollo en ciberseguridad

3.6.5.2.1. Crear un Foro de la Industria de Ciberseguridad para establecer diálogo regular entre los actores de la industria y el MITIC, permitiendo la discusión de temas de interés común y la colaboración en soluciones para fortalecer el ecosistema de ciberseguridad, fomentar la innovación y mejorar la resiliencia frente a las amenazas, con énfasis en la prevención de violencia digital basada en género.

3.6.5.2.2. Fomentar la investigación y desarrollo (I+D) en tecnologías emergentes aplicables a la ciberseguridad nacional, a través de alianzas estratégicas para proyectos de I+D en colaboración con universidades y centros de innovación tecnológica. Se lanzarán convocatorias públicas para el desarrollo de soluciones en IA, blockchain, IoT, y otras tecnologías emergentes aplicadas a la ciberseguridad.

3.6.5.2.3. Establecer alianzas estratégicas con proveedores tecnológicos clave, asegurando el soporte técnico, la actualización continua y la transferencia de conocimiento. Estas alianzas se formalizarán mediante memorandos de entendimiento (MoU) que establezcan compromisos de soporte a largo plazo y la adopción de mejores prácticas en el desarrollo de soluciones de ciberseguridad.

3.6.6. Estar preparados y ciber resilientes

Mejorar la protección de las Infraestructuras de Información Críticas Nacionales (IICN) y aumentar la capacidad de recuperación ante ataques cibernéticos, asegurando el funcionamiento continuo de servicios vitales.

3.6.6.1. Fortalecer equipos de respuesta en ciberseguridad

3.6.6.1.1. Ampliar las capacidades técnicas y humanas del CERT-PY mejorando los procesos de contratación de personal especializado y la adquisición de tecnología avanzada para mejorar la capacidad de respuesta ante incidentes cibernéticos. Esto incluirá la implementación de programas de formación continua y la revisión periódica de protocolos de respuesta rápida para la gestión efectiva de incidentes a nivel nacional.

3.6.6.1.2. Establecer un Centro de Operaciones de Seguridad Nacional (SOC-PY), encargado del manejo centralizado de monitoreo y protección de la infraestructura de TI de OEE las 24 horas del día, los 7 días de la semana y de la coordinación de investigaciones sobre ataques a infraestructuras críticas. El SOC-PY será equipado con tecnologías de monitoreo avanzado, análisis forense y trabajará coordinadamente con el CERT-PY para dar respuesta a incidentes y coordinar acciones entre las entidades públicas y privadas.

3.6.6.1.3. Fortalecer la centralización de la gestión de incidentes en el CERT-PY y el SOC-PY, para unificar la respuesta de múltiples organismos y garantizar una comunicación fluida y la colaboración interinstitucional. Este centro será el punto de contacto único para la gestión de incidentes cibernéticos que involucren infraestructuras críticas y otros sistemas sensibles.

3.6.6.1.4. Desarrollar un sistema nacional de monitoreo y alertas tempranas para la identificación y análisis continuo de amenazas cibernéticas, utilizando herramientas de inteligencia artificial y análisis predictivo que permitan detectar y prevenir incidentes antes de que afecten los sistemas críticos del país.

3.6.6.1.5. Crear un sistema integral de análisis y gestión de vulnerabilidades en los sistemas de software gubernamentales, asegurando la corrección rápida de vulnerabilidades mediante la implementación de herramientas automatizadas de escaneo y el establecimiento de protocolos de respuesta inmediata.

3.6.6.1.6. Implementar un Servicio Nacional de Investigaciones Forenses en Ciberseguridad, dependiente del CERT-PY, con la capacidad de realizar análisis forenses de incidentes cibernéticos tanto de forma remota como in situ. Este servicio estará encargado de identificar la causa raíz de los ataques, recolectar pruebas digitales y colaborar con las autoridades legales para llevar a cabo acciones judiciales cuando sea necesario.

3.6.6.1.7. Invertir en soluciones tecnológicas avanzadas para la protección de sistemas críticos gubernamentales, priorizando tecnologías como sistemas de detección de intrusiones, inteligencia artificial para la ciberseguridad, y plataformas de gestión de incidentes, que fortalezcan la resiliencia de las infraestructuras críticas.

3.6.6.1.8. Centralizar la adquisición de soluciones de ciberseguridad para infraestructuras gubernamentales críticas, creando una plataforma de adquisición conjunta que permita una evaluación estandarizada de soluciones tecnológicas, asegurando compatibilidad y eficacia en todas las entidades públicas.

3.6.6.1.9. Promover la adopción de la metodología DevSecOps en las entidades públicas, integrando la seguridad en cada fase del ciclo de vida del desarrollo de software, mediante la creación de guías prácticas y capacitaciones específicas para los equipos de desarrollo y seguridad de las instituciones gubernamentales.

3.6.6.1.10. Establecer un programa continuo de diagnósticos y auditorías de seguridad para todas las instituciones públicas, asegurando la identificación proactiva de vulnerabilidades y la conformidad con los estándares nacionales e internacionales de ciberseguridad. Este programa incluirá auditorías anuales y evaluaciones de cumplimiento para todas las entidades del gobierno.

3.6.6.1.11. Integrar operativamente al Ministerio de Defensa Nacional, la Fuerzas Armadas de la Nación y a la Secretaría Nacional de Inteligencia en el sistema nacional de ciberseguridad, mediante protocolos claros que definan funciones, cadenas de mando y mecanismos de respuesta conjunta ante amenazas cibernéticas complejas. Complementar las funciones del MITIC y el CERT-PY con capacidades militares especializadas en guerra electrónica, bajo estricta supervisión civil y judicial. Establecer un Centro Nacional de Operaciones Cibernéticas de naturaleza multiagencial, que permita consolidar vigilancia, inteligencia, análisis técnico y respuesta coordinada frente a ataques de alto impacto.

3.6.6.2. Liderar la gestión de crisis cibernéticas con una respuesta coordinada y eficaz

3.6.6.2.1. Desarrollar e implementar una Directiva Nacional de Gestión y Respuesta a Crisis y Emergencias Cibernéticas, que establezca procedimientos claros para la coordinación interinstitucional y la activación de equipos de respuesta rápida ante incidentes cibernéticos de alto impacto. Este protocolo incluirá manuales operativos detallados, líneas de comunicación para la notificación de incidentes y escalas de gravedad para priorizar la respuesta ante diferentes tipos de amenazas.

3.6.6.2.2. Desarrollar una Guía Nacional para la Realización de Ejercicios y Simulacros de Ciberseguridad, que sirva como guía para organizar simulacros regulares a nivel nacional e interinstitucional. Este manual proporcionará metodologías estandarizadas para la planificación, ejecución y evaluación de simulacros que involucren escenarios realistas de ciberamenazas, permitiendo medir la preparación de las infraestructuras críticas y los servicios esenciales para responder a incidentes cibernéticos.

3.6.6.2.3. Establecer un protocolo interinstitucional de coordinación entre entidades de Gobierno ante crisis o amenazas cibernéticas complejas.

3.6.6.3. Defender y proteger la Infraestructura de Información Crítica Nacional (IICN)

3.6.6.3.1. Establecer un marco normativo para la definición de IICN, identificando las entidades propietarias o responsables de la operación de dicha infraestructura, así como los sectores que componen la IICN.

3.6.6.3.2. Delimitar los sectores estratégicos de la IICN mediante un análisis sectorial que permita una clasificación y priorización conforme a su relevancia para la seguridad nacional y el bienestar económico del país.

3.6.6.3.3. Mapear y documentar las entidades propietarias o que operan la IICN en cada sector, asegurando una clara identificación de los actores clave para la protección de la IICN.

3.6.6.3.4. Designar una entidad líder en cada sector de IICN, con la responsabilidad de coordinar los esfuerzos de ciberseguridad y asegurar el cumplimiento de los estándares establecidos a nivel sectorial.

3.6.6.3.5. Fomentar la elaboración de un código de prácticas sectorial para la protección de la IICN, estableciendo medidas, estándares, y procedimientos que garanticen su resiliencia y seguridad frente a amenazas, aplicable a todas las entidades propietarias u operadoras de dicha infraestructura.

3.6.6.3.6. Impulsar la realización de evaluaciones de riesgos cibernéticos en todos los sectores de IICN, asegurando que las entidades propietarias u operadoras implementen evaluaciones periódicas alineadas con el código de prácticas establecido para cada sector.

3.6.6.3.7. Promover la realización de auditorías periódicas para evaluar el nivel de cumplimiento de las entidades propietarias u operadoras de IICN, con el fin de identificar áreas de mejora y garantizar la aplicación efectiva de los estándares de ciberseguridad.

3.6.6.3.8. Elaborar y poner en marcha Planes de Contingencia y Recuperación para IICN, asegurando que todas las entidades propietarias o que operan la IICN cuenten con estrategias de continuidad de negocio y procedimientos de recuperación ante incidentes.

3.6.6.3.9. Realizar ejercicios de simulación de ciberseguridad dirigidos a evaluar la capacidad de respuesta de los propietarios y operadores de IICN, con el objetivo de probar y mejorar la preparación ante incidentes y amenazas cibernéticas.

3.6.7. Unidos contra el Cibercrimen y el Ransomware

Fortalecer la capacidad para combatir el cibercrimen y manejar adecuadamente las pruebas digitales, protegiendo a toda la sociedad contra la ciberdelincuencia.

3.6.7.1. Combatir el cibercrimen con determinación

3.6.7.1.1. Fortalecer el marco legal contra el cibercrimen mediante la adhesión de los compromisos internacionales, así como la implementación de estándares internacionales reconocidos en la materia. Para ello, se diseñará e implementará un plan de acción legislativo que asegure la rápida adaptación de los procedimientos legales a las normas internacionales, y desarrollando una campaña de difusión para sensibilizar a las instituciones

judiciales y fuerzas del orden sobre su relevancia.Impulsar la actualización del marco procesal y sustantivo nacional, incorporando la tipificación precisa de delitos cibernéticos y alineándolo con las mejores prácticas internacionales, e incluyendo la revisión y modificación del código penal y procesal penal, con un enfoque específico en delitos como el acceso ilícito, fraude cibernético y distribución de malware.

3.6.7.1.2. Desarrollar capacidades especializadas para la recolección y análisis de evidencia digital en procesos judiciales, a través de la creación de laboratorios forenses especializados y la adquisición de herramientas avanzadas de análisis digital. Se establecerán protocolos de cadena de custodia para garantizar la validez de las pruebas en procedimientos legales.

3.6.7.1.3. Capacitar a jueces, fiscales y fuerzas del orden en cibercrimen y manejo de evidencia digital, mediante la implementación de un programa de formación continua, que incluirá talleres, cursos especializados y certificaciones internacionales. Este programa será desarrollado en colaboración con organizaciones internacionales y académicas.

3.6.7.1.4. Implementar programas de prevención y educación pública sobre cibercrimen, diseñando campañas masivas de sensibilización dirigidas a la ciudadanía y sectores vulnerables. Estos programas incluirán materiales educativos en línea, seminarios y talleres comunitarios que promuevan el uso seguro de las tecnologías y la reducción de la incidencia de delitos cibernéticos. Adicionalmente, incluirán contenidos para prevenir la violencia de género en línea.

3.6.7.1.5. Fortalecer las unidades policiales especializadas en cibercrimen, dotadas de recursos humanos capacitados y tecnologías avanzadas, para la investigación y persecución de delitos cibernéticos. Estas unidades contarán con tecnologías de monitoreo y análisis forense, así como alianzas estratégicas con organismos internacionales de seguridad.

3.6.7.1.6. Fortalecer la Unidad Especializada de Delitos Informáticos en el Ministerio Público para mejorar su capacidad operativa, incluyendo la contratación de personal especializado en cibercrimen y análisis forense digital, así como la adquisición de herramientas avanzadas de investigación cibernética.

3.6.7.1.7. Fortalecer la cooperación internacional en cibercrimen, facilitando el intercambio de información y la asistencia mutua en investigaciones mediante la adhesión a acuerdos internacionales de cooperación y la creación de canales seguros de comunicación para la colaboración entre autoridades nacionales e internacionales.

3.6.7.2. Hacer frente al ransomware con estrategias sólidas y coordinadas

3.6.7.2.1. Desarrollar e implementar un Marco Integral para la Acción contra el Ransomware, que ofrezca un conjunto de directrices y herramientas para mejorar la capacidad de respuesta y preparación de las organizaciones frente a ataques de ransomware, incluyendo guías de prevención para que las organizaciones fortalezcan sus defensas, protocolos de respuesta

rápida para incidentes de ransomware, y un manual de respuesta a ransomware que estará disponible para todas las organizaciones públicas y privadas.

3.6.7.2.2. Fortalecer la cooperación internacional con otros países y organizaciones internacionales para combatir el Ransomware, estableciendo acuerdos bilaterales y multilaterales que faciliten el intercambio de inteligencia sobre amenazas cibernéticas y las mejores prácticas de prevención y respuesta a estos ataques.

4. INTERVENCIONES PÚBLICAS

Paraguay tendrá una estrategia que facilitará la conversación con los diferentes actores a nivel nacional e internacional para impulsar las apuestas estratégicas del país alrededor de la ciberseguridad. También se constituirá como un referente de política que seguirá evolucionando y fortaleciéndose con nuevas acciones de acuerdo con las prioridades, desafíos y retos futuros que se presenten frente a la ciberseguridad en el país.

A continuación, se presentan las intervenciones públicas de corto, mediano y largo plazo teniendo en cuenta el marco estratégico de la Estrategia Nacional de Ciberseguridad 2025-2028 de Paraguay.

Objetivo 1. Construir juntos un Paraguay ciberseguro
Línea Estratégica 1.1. Consolidar una gobernanza nacional fuerte y cohesionada en ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
1.1.1	Realizar una evaluación exhaustiva del modelo de gobernanza del Sistema Nacional de Ciberseguridad y proponer e implementar modificaciones para adaptarlo al nuevo contexto nacional e internacional.	Informe de evaluación y propuesta de modificaciones elaborado y aprobado	Verificación de la existencia del informe y registro de aprobación	Corto	6 meses	MITIC
1.1.2	Desarrollar e implementar un plan de implementación del Modelo de Gobernanza coordinado liderado por MITIC, el Coordinador Nacional de	Plan de implementación del Modelo de Gobernanza aprobado e implementado	Porcentaje de cumplimiento de las actividades del plan	Corto	3 meses para desarrollo, 36 meses para implementación	MITIC con apoyo del MDN y el MI

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
	Ciberseguridad y el CERT-PY con cronogramas, responsabilidades e indicadores de desempeño.					
1.1.3	Diseñar y lanzar una plataforma digital de participación ciudadana y colaboración interinstitucional en ciberseguridad.	Plataforma digital operativa y en uso	Número de usuarios registrados y participaciones mensuales	Mediano	12 meses	MITIC
1.1.4	Desarrollar y ejecutar un plan integral de fortalecimiento institucional para la autoridad nacional de ciberseguridad.	Plan de fortalecimiento institucional implementado	Porcentaje de cumplimiento de las actividades del plan	Mediano	18 meses	MITIC
1.1.5	Crear e implementar canales de comunicación seguros entre las partes interesadas en ciberseguridad, incluyendo una red nacional de intercambio de información.	Red nacional de intercambio de información operativa	Número de entidades participantes y volumen de información intercambiada	Mediano	12 meses	CERT-PY con apoyo de MDN y MI
1.1.6	Lanzar campañas nacionales e integrales de concienciación en ciberseguridad dirigidas a diversos públicos objetivos.	Campañas de concienciación implementadas	Número de personas concientizadas y encuestas de impacto	Largo	36 meses (campañas continuas)	MITIC en coordinación con el MEC y MINNA
1.1.7	Desarrollar y poner en marcha un sistema de reportes periódicos sobre el progreso y la efectividad en la implementación de la Estrategia Nacional de Ciberseguridad 2025-2028.	Sistema de reportes implementado	Número de informes publicados y nivel de acceso público	Largo	6 meses para desarrollo, 36 meses para implementación	MITIC

Objetivo 1. Construir juntos un Paraguay ciberseguro
Línea Estratégica 2.1. Impulsar una cooperación internacional dinámica y efectiva en ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
1.2.1	Incorporar la ciberseguridad como pilar central de la Política Exterior y agenda diplomática e internacional del país	Estrategia de ciberseguridad para negociaciones internacionales desarrollada y aprobada	Verificación de la existencia del documento de estrategia aprobado	Corto	6 meses	MRE en coordinación con MITIC
1.2.2	Contribuir activamente en foros internacionales clave sobre ciberseguridad	Número de propuestas nacionales presentadas y reuniones en grupos de trabajo	Registro de participaciones y contribuciones en foros internacionales	Mediano	Continuo (evaluación anual)	MRE en coordinación con MITIC
1.2.3	Establecer acuerdos bilaterales de cooperación en ciberseguridad con países estratégicos	Número de acuerdos establecidos y marcos operativos implementados	Registro de acuerdos firmados y evaluación de su implementación	Mediano	24 meses	MRE en coordinación con MITIC.
1.2.4	Definir y promover una postura nacional sobre conducta responsable en el ciberespacio	Documento de postura nacional elaborado y difundido	Verificación del documento y registro de instancias de difusión	Corto	12 meses	MRE en coordinación con MITIC.
1.2.5	Impulsar medidas de fomento de la confianza en el ciberespacio	Estrategia de implementación de medidas de fomento de la confianza desarrollada	Verificación de la estrategia y evaluación de su implementación	Mediano	18 meses para desarrollo, implementación continua	MRE en coordinación con MITIC

Objetivo 2. Invertir en nuestro futuro digital

Línea Estratégica 2.1. Asignar de manera eficiente los recursos actuales de ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
2.1.1	Realizar una evaluación de la inversión pública en ciberseguridad en los OEE	Informe de evaluación elaborado y aprobado	Verificación de la existencia del informe y registro de aprobación	Corto	6 meses	MITIC en coordinación con el MEF
2.1.2	Elaborar una Guía para la Formulación de Proyectos de Inversión Pública de Ciberseguridad	Guía elaborada y aprobada	Verificación de la existencia de la guía y registro de aprobación	Corto	4 meses	MITIC en coordinación con MEF

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
2.1.3	Elaborar una Guía para la Evaluación Socioeconómica de Proyectos de Inversión Pública de Ciberseguridad	Guía elaborada y aprobada	Verificación de la existencia de la guía y registro de aprobación	Corto	4 meses	MITIC - DGCPI en coordinación con el MEF
2.1.4	Capacitar a funcionarios en formulación y evaluación de Proyectos de Inversión Pública de Ciberseguridad	Número de funcionarios capacitados	Registro de asistencia y evaluaciones de los cursos	Mediano	12 meses (programa continuo)	MITIC en coordinación con el MEF
2.1.5	Realizar auditorías periódicas en los OEE sobre recursos de ciberseguridad	Número de auditorías realizadas	Informes de auditoría presentados	Largo	36 meses (auditorías anuales)	CGR en coordinación con MITIC

Objetivo 2. Invertir en nuestro futuro digital
Línea Estratégica 2.2. Movilizar nuevos recursos para la ciberseguridad nacional

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
2.2.1	Crear un mecanismo formal de alianzas público-privadas para proyectos de ciberseguridad	Mecanismo implementado y operativo	Verificación de la existencia del mecanismo y número de alianzas formalizadas	Mediano	12 meses	MITIC en coordinación con el MIC
2.2.2	Diseñar y proponer un esquema de incentivos fiscales y financieros para inversiones en ciberseguridad	Propuesta de esquema de incentivos elaborada y presentada	Verificación de la existencia de la propuesta y registro de presentación	Mediano	8 meses	MITIC en coordinación con el MEF
2.2.3	Implementar un programa nacional de formación en gestión financiera para ciberseguridad	Programa de formación diseñado e implementado	Número de personas capacitadas y evaluaciones del programa	Mediano	18 meses	MITIC en coordinación con el MEF y universidades

Objetivo 3. Desarrollar una fuerza laboral especializada en ciberseguridad
Línea Estratégica 3.1. Fortalecer la oferta del mercado laboral en ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
3.1.1	Implementar programas educativos que fomenten la	Número de estudiantes participantes en programas STEM	Registro de participación en programas y actividades	Mediano	24 meses	MEC en coordinación con el MITIC

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
	alfabetización digital y vocaciones STEM					
3.1.2	Crear plataforma de buenas prácticas para promover carreras en ciberseguridad	Plataforma operativa con recursos y casos de éxito	Verificación de la plataforma y estadísticas de uso	Corto	12 meses	MITIC
3.1.3	Lanzar campañas nacionales de sensibilización sobre privacidad y ciberseguridad	Número de personas alcanzadas por las campañas	Métricas de alcance en redes sociales y participación en capacitaciones	Corto	18 meses (campañas continuas)	MITIC en coordinación con el MEC y MINNA
3.1.4	Desarrollar plataforma para identificar y atraer talento en ciberseguridad	Plataforma operativa y número de usuarios registrados	Verificación de la plataforma y estadísticas de uso	Mediano	18 meses	MITIC en coordinación con el MEC y Ministerio de Trabajo, Empleo y Seguridad Social (MTSS)
3.1.5	Crear guías y recursos educativos sobre rutas de aprendizaje y certificaciones en ciberseguridad	Mapa interactivo sobre rutas de aprendizaje y certificaciones en ciberseguridad publicado	Verificación del mapa y estadísticas de consulta	Corto	12 meses	MITIC en coordinación con el MEC
3.1.6	Impulsar la estandarización de currículos en ciberseguridad	Documento de estándares curriculares aprobado	Verificación del documento y nivel de adopción por instituciones educativas	Mediano	24 meses	MEC en coordinación con el MITIC y la ANEAES
3.1.7	Organizar competencias y hackathons nacionales en ciberseguridad	Número de eventos realizados y participantes	Registro de eventos y participación	Largo	36 meses (eventos anuales)	MITIC en coordinación con la academia y el sector privado

Objetivo 3. Desarrollar una fuerza laboral especializada en ciberseguridad
Línea Estratégica 3.2. Impulsar la demanda del mercado laboral en ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
3.2.1	Desarrollar Marco Nacional de Competencias y Roles de Ciberseguridad	Marco desarrollado y publicado en plataforma digital	Verificación de la publicación del marco y estadísticas de acceso	Corto	12 meses	MITIC en coordinación con la academia e industria
3.2.2	Crear e implementar Sistema Nacional de Acreditación de Profesionales de Ciberseguridad	Sistema operativo y número de profesionales acreditados	Registro de acreditaciones otorgadas y renovaciones	Mediano	18 meses	MITIC en coordinación con el MEC
3.2.3	Fortalecer capacidades de OEE para reclutar	Número de OEE que implementan	Encuestas a OEE y registro	Mediano	12 meses	MITIC en coordinación con el MEF

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
	talento en ciberseguridad	nuevas prácticas de reclutamiento	de contrataciones			
3.2.4	Implementar mecanismos de incentivos para promover marcos de trayectoria profesional en ciberseguridad	Número de organizaciones con programas de desarrollo profesional certificados	Registro de certificaciones otorgadas	Mediano	24 meses	MITIC en coordinación con sector privado
3.2.5	Desarrollar programas para promover diversidad en la fuerza laboral de ciberseguridad	Porcentaje de mujeres y minorías en roles de ciberseguridad	Encuestas laborales y registros de participación en programas	Largo	36 meses	MITIC en coordinación con el MM y otras entidades
3.2.6	Diseñar plan nacional para atraer y retener talento en ciberseguridad en OEE	Plan diseñado e implementado	Verificación del plan y medición de indicadores de retención	Mediano	18 meses	MITIC en coordinación con el MEF

Objetivo 4. Establecer y cumplir reglas claras en el ciberespacio
Línea Estratégica 4.1. Impulsar la actualización y modernización del marco legal y regulatorio de ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
4.1.1	Adoptar un estándar oficial de términos y conceptos clave en ciberseguridad	Documento normativo de términos y conceptos aprobado	Verificación de la existencia y aprobación del documento	Corto	6 meses	MITIC
4.1.2	Desarrollar y presentar un proyecto de Ley Marco de Ciberseguridad y Protección de IICN	Proyecto de ley elaborado y presentado al Congreso	Verificación del proyecto de ley y su presentación formal	Mediano	18 meses	MITIC en coordinación con grupo de trabajo multisectorial y Poder Legislativo
4.1.3	Implementar estrategia de incidencia legislativa para la Ley Marco	Número de presentaciones y campañas realizadas	Registro de actividades de incidencia y sensibilización	Mediano	12 meses	MITIC en coordinación con Poder Legislativo
4.1.4	Actualizar y modernizar el marco legal en temas relacionados a ciberseguridad	Número de leyes y regulaciones actualizadas	Registro de modificaciones legales aprobadas	Largo	36 meses	MITIC en coordinación con el Poder Legislativo y otros ministerios relevantes

Objetivo 5. Promover el uso de un lenguaje técnico común
Línea Estratégica 5.1. Establecer y adoptar estándares nacionales sólidos en ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
5.1.1	Desarrollar un marco nacional de estandarización tecnológica	Marco de estandarización desarrollado y publicado	Verificación de la publicación oficial del marco	Corto	12 meses	MITIC
5.1.2	Promover la adopción de estándares y mejores prácticas internacionales	Número de campañas realizadas y portal digital implementado	Registro de campañas y verificación del portal	Mediano	18 meses	MITIC
5.1.3	Establecer políticas nacionales de adquisición y actualización tecnológica	Catálogo de tecnologías recomendadas publicado	Verificación de la publicación del catálogo	Mediano	12 meses	MITIC en coordinación con la DNCP
5.1.4	Implementar programas nacionales para la homologación de sistemas y herramientas	Programa de homologación implementado y centro de pruebas establecido	Número de sistemas homologados y verificación del centro de pruebas	Largo	24 meses	MITIC en coordinación con la CONACYT
5.1.5	Crear e implementar un Sistema de Certificación de Productos y Soluciones Tecnológicas de Ciberseguridad	Sistema de certificación implementado	Número de productos y soluciones certificados	Largo	36 meses	MITIC en coordinación con MEC
5.1.6	Diseñar e implementar un marco de control para la seguridad de la cadena de suministro digital en infraestructura crítica.	Marco nacional de control aprobado y en ejecución	Verificación del marco y cantidad de auditorías realizadas a proveedores estratégicos	Mediano	18 meses	MITIC en coordinación con la DNCP

Objetivo 5. Promover el uso de un lenguaje técnico común
Línea Estratégica 5.2. Fomentar la investigación y el desarrollo en ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
5.2.1	Crear un Foro de la Industria de Ciberseguridad	Foro establecido y número de reuniones realizadas	Acta de constitución del foro y registro de reuniones	Corto	6 meses	MITIC
5.2.2	Fomentar la I+D en tecnologías emergentes aplicables a la ciberseguridad	Número de proyectos de I+D iniciados	Registro de proyectos y convocatorias públicas realizadas	Mediano	24 meses	MITIC en coordinación con la CONACYT y universidades
5.2.3	Establecer alianzas estratégicas con	Número de MoU firmados	Registro de MoU y	Mediano	18 meses	MITIC

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
	proveedores tecnológicos clave		acuerdos de colaboración			

Objetivo 6. Estar preparados y ciber resilientes
Línea Estratégica 6.1. Fortalecer equipos de respuesta en ciberseguridad

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
6.1.1	Ampliar capacidades técnicas y humanas del CERT-PY	Número de personal especializado contratado y tecnologías adquiridas	Registro de contrataciones y adquisiciones	Mediano	18 meses	MITIC
6.1.2	Establecer Centro de Operaciones de Seguridad Nacional del Paraguay (SOC-PY)	SOC-PY operativo 24/7	Verificación de la implementación y operación del SOC-PY	Mediano	24 meses	MITIC
6.1.3	Fortalecer centralización de gestión de incidentes en CERT-PY y SOC-PY	Protocolo de gestión centralizada implementado	Número de incidentes gestionados de manera centralizada	Corto	12 meses	MITIC
6.1.4	Desarrollar sistema nacional de monitoreo y alertas tempranas	Sistema implementado y operativo	Número de alertas generadas y prevenidas	Largo	36 meses	MITIC
6.1.5	Crear sistema integral de análisis y gestión de vulnerabilidades	Sistema implementado y operativo	Número de vulnerabilidades identificadas y corregidas	Mediano	18 meses	MITIC
6.1.6	Implementar Servicio Nacional de Investigaciones Forenses en Ciberseguridad	Servicio operativo y realizando análisis forenses	Número de análisis forenses realizados	Largo	24 meses	MITIC - DGCPI en coordinación con CERT-PY
6.1.7	Invertir en soluciones tecnológicas avanzadas para protección de sistemas críticos	Soluciones implementadas en sistemas críticos	Porcentaje de sistemas críticos protegidos con nuevas tecnologías	Mediano	24 meses	MITIC - DGCPI en coordinación con CERT-PY
6.1.8	Centralizar adquisición de soluciones de ciberseguridad	Plataforma de adquisición conjunta implementada	Número de adquisiciones realizadas a través de la plataforma	Corto	12 meses	MITIC - DGCPI en coordinación con DNCP
6.1.9	Promover adopción de metodología DevSecOps	Guías y capacitaciones desarrolladas	Número de entidades que adoptan DevSecOps	Mediano	18 meses	MITIC - DGCPI en coordinación con CERT-PY
6.1.10	Establecer programa de diagnósticos y auditorías de seguridad	Programa implementado	Número de auditorías realizadas anualmente	Largo	36 meses (programa continuo)	MITIC - DGCPI en coordinación con CERT-PY

Objetivo 6. Estar preparados y ciber resilientes
Línea Estratégica 6.2. Liderar la gestión de crisis cibernéticas con una respuesta coordinada y eficaz

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
6.2.1	Desarrollar e implementar Directiva Nacional de Gestión y Respuesta a Crisis y Emergencias Cibernéticas	Directiva desarrollada y aprobada	Verificación de la existencia y aprobación de la directiva	Corto	12 meses	MITIC en coordinación con el, MDN, DSIRMIL, DIGETIC, MI, PN.
6.2.2	Desarrollar Guía Nacional para la Realización de Ejercicios y Simulacros de Ciberseguridad	Guía desarrollada y publicada	Verificación de la existencia y publicación de la guía	Corto	9 meses	MITIC en coordinación con el MDN, DSIRMIL, DIGETIC, MI, PN.
6.2.3	Establecer un protocolo interinstitucional de coordinación entre MITIC, Fuerzas Armadas, SNI y otras entidades ante amenazas cibernéticas complejas.	Protocolo operativo aprobado e implementado	Verificación del documento aprobado y registro de ejercicios conjuntos realizados	Mediano	18 meses	MITIC en coordinación con MDN, DIGETIC, SNI y el MI.
6.2.4	Crear un Centro Nacional de Operaciones Cibernéticas con participación de MITIC, CERT-PY, FF.AA., SNI y otros actores clave para respuesta técnica coordinada.	Centro operativo establecido y en funcionamiento	Verificación de funcionamiento, cantidad de incidentes gestionados de forma conjunta	Largo	36 meses	MITIC en coordinación con el MDN, SNI, MI y otras agencias.

Objetivo 6. Estar preparados y ciber resilientes
Línea Estratégica 6.3.

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
6.3.1	Establecer marco normativo para definición de IICN	Marco normativo aprobado	Verificación de la existencia y aprobación del marco	Corto	12 meses	MITIC
6.3.2	Delimitar sectores estratégicos de IICN	Documento de clasificación y priorización de sectores IICN	Verificación del documento y su aprobación	Corto	6 meses	MITIC
6.3.3	Mapear entidades propietarias/operadoras de IICN	Mapa de entidades IICN por sector	Verificación del mapa y su	Mediano	12 meses	MITIC en coordinación

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
			actualización periódica			con entidades sectoriales
6.3.4	Designar entidad líder por sector IICN	Resolución de designación de entidades líderes	Verificación de resoluciones emitidas	Corto	3 meses	MITIC
6.3.5	Elaborar código de prácticas sectorial para IICN	Código de prácticas aprobado por sector	Número de códigos sectoriales aprobados	Mediano	18 meses	Entidades líderes sectoriales con apoyo de MITIC
6.3.6	Realizar evaluaciones de riesgos cibernéticos en IICN	Porcentaje de entidades IICN con evaluación de riesgos	Registro de evaluaciones realizadas	Largo	24 meses (proceso continuo)	Entidades propietarias / operadoras IICN
6.3.7	Implementar auditorías periódicas de cumplimiento	Número de auditorías realizadas	Informes de auditoría presentados	Largo	36 meses (auditorías anuales)	MITIC
6.3.8	Elaborar Planes de Contingencia y Recuperación	Porcentaje de entidades IICN con planes aprobados	Verificación de planes presentados	Mediano	18 meses	Entidades propietarias / operadoras IICN
6.3.9	Realizar ejercicios de simulación de ciberseguridad	Número de ejercicios realizados por sector	Informes de ejercicios y evaluaciones	Largo	36 meses (ejercicios anuales)	MITIC en coordinación con entidades sectoriales

Objetivo 7. Unidos contra el Cibercrimen y el Ransomware
Línea Estratégica 7.1. Combatir el cibercrimen con determinación

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
7.1.1	Actualizar el marco procesal y sustantivo nacional en materia de cibercrimen	Marco legal actualizado	Número de leyes y códigos modificados	Mediano	18 meses	MJ en coordinación con el Congreso Nacional
7.1.2	Desarrollar capacidades para recolección y análisis de evidencia digital	Laboratorios forenses implementados y operativos	Número de laboratorios creados y casos atendidos	Mediano	24 meses	MP en coordinación con la PN
7.1.3	Capacitar a jueces, fiscales y fuerzas del orden en cibercrimen	Programa de formación implementado	Número de funcionarios capacitados	Largo	36 meses (programa continuo)	PJ en coordinación con el MP y PN
7.1.4	Implementar programas de prevención y educación pública sobre cibercrimen	Campañas de sensibilización realizadas	Alcance de las campañas y número de personas capacitadas	Mediano	24 meses	MITIC en coordinación con el MEC y el PJ
7.1.5	Fortalecer unidades policiales especializadas en cibercrimen	Unidades fortalecidas y equipadas	Número de unidades creadas /fortalecidas y casos resueltos	Mediano	18 meses	MI - PN
7.1.6	Fortalecer la Unidad Especializada de Delitos Informáticos del Ministerio Público	Unidad fortalecida y equipada	Número de personal especializado contratado y	Corto	12 meses	MP

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
			casos atendidos			
7.1.7	Fortalecer la cooperación internacional en cibercrimen	Acuerdos de cooperación firmados	Número de países con los que Paraguay tiene acuerdos y casos de colaboración	Largo	36 meses (proceso continuo)	MRE en coordinación con el MP

Objetivo 7. Unidos contra el Cibercrimen y el Ransomware
Línea Estratégica 7.2.

N°	Acción	Indicador de Producto	Método de Medición	Plazo	Tiempo de Implementación	Entidad Responsable
7.2.1	Desarrollar e implementar Marco Integral para la Acción contra el Ransomware	Marco desarrollado y publicado	Verificación de la existencia y publicación del marco	Mediano	18 meses	MITIC en coordinación el MRE
7.2.2	Fortalecer la cooperación internacional para combatir el Ransomware	Número de acuerdos de cooperación establecidos	Registro de acuerdos firmados y actividades de cooperación realizadas	Largo	36 meses (proceso continuo)	MITIC en coordinación y el MRE

OEE responsables:

ANEAES	Agencia Nacional de Evaluación y Acreditación de la Educación Superior
CERT-PY	Centro de Respuestas ante Incidentes Cibernéticos del Paraguay
CGR	Contraloría General de la República
CONACYT	Consejo Nacional de Ciencia y Tecnología
DIGETIC	Dirección General de Tecnologías de la Información y Comunicación de las Fuerzas Armadas
DCIRMIL	División de respuestas a incidentes cibernéticos militares de las Fuerzas Armadas
DNCP	Dirección Nacional de Contrataciones Públicas
MDN	Ministerio de Defensa Nacional
MI	Ministerio del Interior
MEC	Ministerio de Educación y Ciencias
MEF	Ministerio de Economía y Finanzas
MIC	Ministerio de Industria y Comercio
MITIC	Ministerio de Tecnologías de la Información y Comunicación
MITIC - DGCPI	Dirección General de Ciberseguridad y Protección de la Información del MITIC
MJ	Ministerio de Justicia
MM	Ministerio de la Mujer
MINNA	Ministerio de la Niñez y la Adolescencia
MRE	Ministerio de Relaciones Exteriores
MTSS	Ministerio de Trabajo, Empleo y Seguridad Social
ONA	Organismo Nacional de Acreditación
PN	Policía Nacional

5. SEGUIMIENTO, EVALUACIÓN Y GESTIÓN DE RIESGOS

El seguimiento a la ejecución física y presupuestal de las acciones propuestas para el cumplimiento de los Objetivos Estratégicos se realizará a través de un *Plan de Acción* que

señala las entidades responsables de cada acción, los períodos de ejecución de estas, los recursos necesarios y disponibles para llevarlas a cabo, y la importancia de cada acción para el cumplimiento del propósito general y los objetivos específicos bajo cada pilar de la Estrategia.

El MITIC informará periódicamente actividades de monitoreo y evaluación de la implementación de la Estrategia y presentará reportes anuales.

Paraguay adelantará monitoreo del nivel de madurez en ciberseguridad y evaluación de las capacidades de las múltiples partes interesadas con el fin de asegurar una mejora continua, haciendo énfasis en el corto y mediano plazo. Adicionalmente, se soportará en el desarrollo de auditorías sobre los procesos que llevan a cabo las instituciones públicas y el desarrollo de ejercicios de eficiencia comparativa basada en la recolección y análisis de información estadística relevante a nivel nacional, así como en la elaboración de reportes situacionales sobre el estado de la ciberseguridad.

Finalmente, se prevé también la revisión y la actualización de la Estrategia cada cuatro años o según sea necesario.

6. REFERENCIAS BIBLIOGRÁFICAS

CAF. (2024). *Hacia el cierre de la brecha digital.* Obtenido de https://scioteca.caf.com/handle//123456789/2272

CERT-PY. (2019). *Estado de la Ciberserguridad en Paraguay - Año 2019.* Obtenido de https://www.cert.gov.py/wp-content/uploads/2022/02/Informe_Ciberseguridad_Paraguay_2019_-_final.pdf

CERT-PY. (2020). *Estado de la Ciberseguridad en Paraguay - Año 2020.* Obtenido de https://www.cert.gov.py/wp-content/uploads/2022/02/Informe_Ciberseguridad_Paraguay_2020_-_final-2.pdf

CERT-PY. (2022). *Estado de la Ciberseguridad en Paraguay - Año 2022.* Obtenido de https://www.cert.gov.py/wp-content/uploads/2024/01/Informe-Ciberseguridad-Paraguay-2022.pdf

CONATEL. (2024). *Avances al Segundo Semestre de 2023 del PNT 21-25.* Obtenido de https://www.conatel.gov.py/conatel/wp-content/uploads/2024/07/informe-avance-objetivos-pnt-21-25-segundo-semestre-2023_final.pdf

CSIRT Americas Network. (2024). *CSIRT Americas Network*. Obtenido de https://www.csirtamericas.org/

e-Governance Academy. (2024). *National Cyber Security Index Project.* Obtenido de https://ncsi.ega.ee/ncsi-index/

FORTINET. (2024). *Outbreak Alerts Annual Report 2023.* Obtenido de https://global.fortinet.com/lp-en-ap-outbreakalerts-report?utm_content=website

GCSCC. (2024). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Obtenido de https://gcscc.ox.ac.uk/the-cmm

ITU. (2022). Obtenido de ITU Facts and Figures 2022: https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-internet-use-in-urban-and-rural-areas/

ITU. (2023a). Obtenido de ITU Facts and Figures 2023 - Internet Use: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

ITU. (2023b). *Global Cybersecurity Index (GCI) 4th Edition*. Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU. (2024). *Global Cybersecurity Index 2024 5th Edition.* Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Ministerio de Relaciones Exteriores de Paraguay. (2024). *Tratados Internacionales de Paraguay*. Obtenido de https://www.mre.gov.py/tratados/public_web/Tratados.aspx

MITIC. (2022). *Plan Nacional TIC 2023-2030.* Obtenido de https://mitic.gov.py/plan-nacional-de-tic-2022-2030/

OEA & BID. (2020). *Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Obtenido de https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

SENATICs. (2017). *Plan Nacional de Ciberseguridad 2017 de Paraguay.* Obtenido de https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

WEF. (2024). *The Global Risks Report 2024.* Obtenido de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf?_gl=1*183q1hb*_up*MQ..&gclid=CjwKCAjw6c63BhAiEiwAF0EH1Dt3nKH9ZPLwl6AXtnOnDyzg-P-RAyWCz9L8e3AeVgB37sxFbTnH4hoCckkQAvD_BwE

ANEXO 1

Marco normativo en materia de ciberseguridad en Paraguay

Cuadro 8. Principales acuerdos internacionales relacionados

Título	Tipo	Organismo	Fecha
CARTA DE LAS NACIONES UNIDAS ENMIENDA AL ARTÍCULO 61 DE LA CARTA DE LAS NACIONES UNIDAS ENMIENDA AL ARTÍCULO 109 DE LAS NACIONES UNIDAS ENMIENDAS A LOS ARTÍCULOS 23, 27, Y 61 DE LA CARTA DE LAS NACIONES UNIDAS DECLARACIONES DE ACEPTACIÓN DE LAS OBLIGACIONES CONSIGNADAS EN LA CARTA DE LAS NACIONES UNIDAS	MULTILATERAL	ONU	26/06/1945
CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO RELATIVO A LA VENTA DE NIÑOS, LA PROSTITUCIÓN INFANTIL Y LA UTILIZACIÓN DE NIÑOS EN LA PORNOGRAFÍA. PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO RELATIVO A UN PROCEDIMIENTO DE COMUNICACIONES ENMIENDA AL PÁRRAFO 2 DEL ARTÍCULO 43 DE LA CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO	MULTILATERAL	ONU	4/4/1990
CONVENCIÓN SOBRE LOS DERECHOS DE LAS PERSONAS CON DISCAPACIDAD. PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LOS DERECHOS DE LAS PERSONAS CON DISCAPACIDAD.	MULTILATERAL	ONU	30/03/2007
CONVENCIÓN INTERNACIONAL SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN RACIAL ENMIENDA AL ARTÍCULO 8 DE LA CONVENCIÓN INTERNACIONAL SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN RACIAL	MULTILATERAL	ONU	13/09/2000
CONVENCIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN CONTRA LA MUJER PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN CONTRA LA MUJER ENMIENDA AL PÁRRAFO 1 DEL ARTÍCULO 20 DE LA CONVENCIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN CONTRA LA MUJER	MULTILATERAL	ONU	
ESTATUTO DE ROMA DE LA CORTE PENAL INTERNACIONAL	MULTILATERAL	ONU	7/10/1998
CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA DELINCUENCIA ORGANIZADA TRANSNACIONAL. CONVENCIÓN DE PALERMO	MULTILATERAL	ONU	
CONVENCIÓN DE VIENA SOBRE EL DERECHO DE LOS TRATADOS	MULTILATERAL	ONU	23/05/1969
CONVENCIÓN DE VIENA SOBRE LA REPRESENTACIÓN DE LOS ESTADOS EN SUS RELACIONES CON LAS ORGANIZACIONES INTERNACIONALES DE CARÁCTER UNIVERSAL	MULTILATERAL	ONU	
TRATADO SOBRE LA PROHIBICIÓN DE LAS ARMAS NUCLEARES	MULTILATERAL	ONU	20/09/2017
TRATADO SOBRE EL COMERCIO DE ARMAS	MULTILATERAL	ONU	19/06/2013
ESTATUTO DE LA CORTE INTERNACIONAL DE JUSTICIA	MULTILATERAL	ONU	26/06/1945
PROTOCOLO FACULTATIVO DEL PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS.	MULTILATERAL	ONU	
PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS.	MULTILATERAL	ONU	
CARTA DE LA ORGANIZACIÓN DE ESTADOS AMERICANOS	MULTILATERAL	OEA	
CONVENCIÓN INTERAMERICANA CONTRA EL TERRORISMO	MULTILATERAL	OEA	
CONVENCION INTERAMERICANA SOBRE ASISTENCIA MUTUA EN MATERIA PENAL PROTOCOLO FACULTATIVO RELATIVO A LA CONVENCIÓN INTERAMERICANA SOBRE ASISTENCIA MUTUA EN MATERIA PENAL.	MULTILATERAL	OEA	
CONVENCIÓN INTERAMERICANA PARA PREVENIR, SANCIONAR Y ERRADICAR LA VIOLENCIA CONTRA LA MUJER (CONVENCIÓN DE BELÉM DO PARÁ)	MULTILATERAL	OEA	17/10/1995

Título	Tipo	Organismo	Fecha
CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS - PACTO DE SAN JOSÉ DE COSTA RICA	MULTILATERAL	OEA	22/11/1969
CONVENCIÓN INTERAMERICANA SOBRE CONCESIÓN DE LOS DERECHOS POLÍTICOS A LA MUJER	MULTILATERAL	OEA	20/08/1951
CONVENCIÓN INTERAMERICANA SOBRE CONCESIÓN DE LOS DERECHOS CIVILES A LA MUJER	MULTILATERAL	OEA	2/5/1948
ACUERDO SOBRE RECONOCIMIENTO MUTUO DE MEDIDAS DE PROTECCIÓN PARA LAS MUJERES EN SITUACIÓN DE VIOLENCIA DE GÉNERO ENTRE LOS ESTADOS PARTE DEL MERCOSUR Y ESTADOS ASOCIADOS	MULTILATERAL	MERCOSUR	20/07/2022
ACUERDO DE RECONOCIMIENTO MUTUO DE CERTIFICADOS DE FIRMA DIGITAL DEL MERCOSUR	MULTILATERAL	MERCOSUR	5/12/2019
ACUERDO PARA LA ELIMINACIÓN DEL COBRO DE CARGOS DE ROAMING INTERNACIONAL A LOS USUARIOS FINALES DEL MERCOSUR	MULTILATERAL	MERCOSUR	17/07/2019
ACUERDO MARCO DE COOPERACIÓN ENTRE LOS ESTADOS PARTE DEL MERCOSUR Y ESTADOS ASOCIADOS PARA LA CREACIÓN DE EQUIPOS CONJUNTOS DE INVESTIGACIÓN	MULTILATERAL	MERCOSUR	2/8/2010
ACUERDO ENTRE LOS ESTADOS PARTE DEL MERCOSUR Y ESTADOS ASOCIADOS SOBRE COOPERACIÓN REGIONAL PARA LA PROTECCIÓN DE LOS DERECHOS DE NIÑOS, NIÑAS Y ADOLESCENTES EN SITUACIÓN DE VULNERABILIDAD	MULTILATERAL	MERCOSUR	30/06/2008
ACUERDO PARA LA IMPLEMENTACIÓN DE BASES DE DATOS COMPARTIDAS DE NIÑOS, NIÑAS Y ADOLESCENTES EN SITUACIÓN DE VULNERABILIDAD DEL MERCOSUR Y ESTADOS ASOCIADOS	MULTILATERAL	MERCOSUR	30/06/2008
PROTOCOLO DE ASUNCIÓN SOBRE COMPROMISO CON LA PROMOCIÓN Y PROTECCIÓN DE LOS DERECHOS HUMANOS DEL MERCOSUR (Ley Nº 3034)	MULTILATERAL	MERCOSUR	20/06/2005
ACUERDO MARCO SOBRE COOPERACIÓN EN MATERIA DE SEGURIDAD REGIONAL ENTRE LOS ESTADOS PARTE DEL MERCOSUR, BOLIVIA Y CHILE (Ley N° 2887)	MULTILATERAL	MERCOSUR	16/12/2004
ACUERDO MARCO SOBRE COOPERACIÓN EN MATERIA DE SEGURIDAD REGIONAL ENTRE LOS ESTADOS PARTE DEL MERCOSUR	MULTILATERAL	MERCOSUR	16/12/2004
ACUERDO DE ASISTENCIA JURÍDICA MUTUA EN ASUNTOS PENALES ENTRE LOS ESTADOS PARTE DEL MERCOSUR, LA REPÚBLICA DE BOLIVIA Y LA REPÚBLICA DE CHILE	MULTILATERAL	MERCOSUR	18/02/2002
MEMORÁNDUM DE ACUERDO ENTRE LA COMUNIDAD EUROPEA Y EL MERCADO COMÚN DEL SUR (MERCOSUR)RELATIVO A LA ORIENTACIÓN PLURIANUALES PARA LA REALIZACIÓN DE LA COOPERACIÓN COMUNITARIA	MULTILATERAL	MERCOSUR	26/07/2001
PROTOCOLO DE ASISTENCIA JURÍDICA MUTUA EN ASUNTOS PENALES	MULTILATERAL	MERCOSUR	25/06/1996
ACUERDO MARCO INTERREGIONAL DE COOPERACIÓN ENTRE EL MERCADO COMÚN DEL SUR Y LA COMUNIDAD EUROPEA	MULTILATERAL	MERCOSUR	15/12/1995
TRATADO PARA LA CONSTITUCIÓN DE UN MERCADO COMÚN (TRATADO DE ASUNCIÓN)	MULTILATERAL	MERCOSUR	30/10/1991
CONVENCIÓN SOBRE LA CIBERDELINCUENCIA PROTOCOLO ADICIONAL AL CONVENIO SOBRE CIBERDELINCUENCIA RELATIVO A LA PENALIZACIÓN DE ACTOS DE ÍNDOLE RACISTA Y XENÓFOBA COMETIDOS POR MEDIO DE SISTEMAS INFORMÁTICOS	MULTILATERAL	CONSEJO DE EUROPA	15/12/2017
CONVENCIÓN SOBRE SEGURIDAD NUCLEAR	MULTILATERAL	OTROS ORGANISMOS	-

Fuente: Elaboración propia a partir de (Ministerio de Relaciones Exteriores de Paraguay, 2024)

Cuadro 9. Marco constitucional, legal y regulatorio relacionado

Tema	Ley	Decretos
Privacidad, libertad de	**Constitución Nacional** de la República del Paraguay	

Tema	Ley	Decretos
expresión y derechos humanos		
Ciberseguridad		Decreto N° **7052/2017** - Aprueba el Plan Nacional de Ciberseguridad de 2017 y se integra la Comisión Nacional de Ciberseguridad
Delito cibernético (sustantiva y procesal)	Ley Nº **5994/2017** - Aprueba la Convención sobre la Ciberdelincuencia y el Protocolo Adicional al Convenio sobre Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos Ley Nº **4439/2011** - Nuevos delitos en Código Penal Ley Nº **1286/1998** - Código Procesal Penal Ley Nº **1160/1997** - Código Penal	
Comercio electrónico / Firma electrónica / Transacciones electrónicas	Ley N° **7121/2023** - Aprueba el acuerdo de reconocimiento mutuo de certificados de firma digital del MERCOSUR Ley N° **7120/2023** - Aprueba el acuerdo sobre comercio electrónico del MERCOSUR Ley N° **6822/2021** - De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos Ley N° **4868/2013** - Ley de Comercio Electrónico	Decreto N° **7576/2022** - Reglamenta la Ley Nº 6822/2021 Decreto N° **1165 /2014** - Reglamenta la Ley N° 4868/2013
Protección al Consumidor	Ley N° **6624/2020** – QUE MODIFICA EL ARTÍCULO 30 DE LA LEY N° 1334/1998 "DE DEFENSA DEL CONSUMIDOR Y DEL USUARIO". Ley N° **1334/1998** - De defensa del consumidor y del usuario.	
Protección de Datos Personales	Ley N° **6534/2020** - De protección de datos personales crediticios	
Tecnologías de la Información y las Comunicaciones	Ley N° **7085/2023** - De inclusión digital para las personas adultas mayores Ley N° **6738/2021** - Establece la modalidad del teletrabajo en relación dependencia Ley N° **6298/2019** - Aprueba el Contrato de Préstamo No. 4650/OC-PR suscrito entre la República del Paraguay y el Banco Interamericano de Desarrollo, hasta por un monto de US$ 130.000.000 para el financiamiento del Programa de Apoyo a la Agenda Digital a cargo de MITIC Ley N° **6207/2018** - Crea el Ministerio de Tecnologías de la Información y Comunicación MITIC	Decreto N° **8942/2023** - Aprueba el Plan Nacional TIC 2022-2030 Decreto N° **2274/2019** - Reglamenta la Ley Nº 6207/2018 Decreto N° **2145/2019** - Crea el Comité Estratégico Digital Decreto N° **1260/2019** - Aprueba la estructura orgánica del MITIC Decreto N° **6234/2016** - Establece la estructura TIC del Gobierno
Protección Infantil en Línea y protección a la mujer	Ley N° **7239/2024** - De emergencia social ante la violencia contra las mujeres, niñas, niños y adolescentes y refuerza estrategias tendientes a promover el cambio de patrones socioculturales que sostienen la desigualdad entre hombres y mujeres Ley N° **5777/2016** - De protección integral a las mujeres contra toda forma de violencia Ley N° **5770/2016** - Aprueba el protocolo facultativo de la convención sobre los derechos del niño relativo a un procedimiento de comunicaciones Ley N° **5653/2016** – De protección de niños, niñas y adolescentes contra contenidos nocivos de Internet Ley N° **57/1990** - Aprueba y ratifica la Convención de las Naciones Unidas sobre los derechos del niño	Decreto N° **8098/2022** - Reglamenta la Ley N° 5653/2016 Decreto N° **6973/2017** - Reglamenta la Ley N° 5777/2016 Resolución SENATICS N° **143/2017** - Especificaciones técnicas mínimas de software de Protección de niños, niñas y adolescentes establecido en la Ley N° 5653/2016 **Resolución SNNA N° 87/2017** Por la cual se describen contenidos nocivos para niños, niñas y adolescentes en el marco de la aplicación de la Ley N° 5653/2016
Propiedad Intelectual	Ley N° **4798/2013** - Crea la Dirección Nacional de Propiedad Intelectual DINAPI	Decreto N° **3074/2019** - Crea el Centro Nacional de Coordinación de Derechos de Propiedad Intelectual

Tema	Ley	Decretos
	Ley N° **1582/2000** - Aprueba el tratado de la 0rganización Mundial de la Propiedad Intelectual OMPI sobre derecho de autor. Ley N° **1224/1986** - Aprueba el convenio que establece la OMPI	Decreto N° **7132/2017** - Aprueba el Plan Nacional de Propiedad Intelectual
Otros	Ley N° **5241/2014** - Crea el Sistema Nacional de Inteligencia	Decreto N° **2812/2014** - Reglamenta la Ley N° 5241/2014

Fuente: Elaboración propia

Cuadro 10. Marco técnico relacionado

Tipo	Número	Propósito
RESOLUCIÓN	MITIC N° **678/2022**	Guía de gestión de cuentas oficiales en redes sociales para OEE y sus autoridades
	MITIC N° **346/2020**	Reporte Obligatorio de Incidentes Cibernéticos por parte los OEE
	MITIC N° **277/2020**	Guía de Controles Críticos de Ciberseguridad
	MITIC N° **218/2020**	Lineamientos del Portal Único de Gobierno y Trámites en Línea
	MITIC N° **733/2019**	Modelo de Gobernanza de Seguridad de la Información
	MITIC N° **699/2019**	Criterios mínimos de seguridad de software
	MITIC N° **432/2019**	Directivas de Ciberseguridad para Medios del Estado

Fuente: Elaboración propia

ANEXO 2

Cuadro 11. Productos esperados de la implementación del Plan Nacional de Ciberseguridad 2017

EJES	PRODUCTOS ESPERADOS
SENSIBILIZACIÓN Y CULTURA	• **Estudios/encuestas** sobre la sensibilización de ciberseguridad • **Campañas temáticas** de sensibilización pública • **Campañas de sensibilización** entre entidades gubernamentales • **Avisos** con recomendaciones de buenas prácticas de ciberseguridad • **Material educativo** para estudiantes • **Módulos educativos de sensibilización** para niños, niñas, padres y escuelas • **Charlas de orientación y capacitación** a niños, jóvenes, adultos y educadores • **Materiales** en formato textual e ilustrativo sobre problemáticas • **Mecanismos que faciliten el reporte** de crímenes cibernéticos que afectan a niños y niñas • **Grupo de Trabajo** para dar asistencia y brindar soporte a víctimas • **Programas de sensibilización** para el nivel ejecutivo y los responsables de toma de decisiones
INVESTIGACIÓN, DESARROLLO E INNOVACIÓN	• **Programas de fomento** al uso de las TIC • **Cursos** en ciberseguridad en malla curricular • **Programas** para docentes • **Becas** y otras oportunidades de capacitación para academia y profesionales • **Programas de capacitación** de talento • **Programas de entrenamiento** en conceptos básicos a organizaciones • **Eventos y talleres** profesionales • **Programas para el fomento de productos y servicios** en materia de TIC y ciberseguridad • **Códigos de conducta y buenas prácticas** en ciberseguridad • **Programas de incentivo** a las MIPYMES • **Sellos de confianza** en línea para fomentar comercio electrónico • **Estándares** de ciberseguridad
PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS	• **Base de datos** de toda la infraestructura crítica • **Normativa** en ciberseguridad para la Protección de Infraestructuras Críticas • **Análisis de riesgo** • **Ejercicios y simulacros** de emergencias • **Directrices técnicas** para la gestión de sistemas de control industrial • **Proyectos** específicos de control industrial y ciberseguridad con otros países • **Reuniones periódicas** entre Ministerio Público y CERT-PY • **Ejercicios de simulación** de incidentes cibernéticos
CAPACIDAD DE RESPUESTA ANTE INCIDENTES CIBERNÉTICOS	• **Base de datos nacional** actualizada de los incidentes • **Convenios de colaboración y cooperación** para el intercambio de información • **Código de Conducta** voluntario para operadores • **Mecanismos de cooperación** entre el CERT-PY y el NIC.PY • **Equipos de respuesta a incidentes** en otros sectores • **Mecanismos** para compartir información de incidentes • **Cursos de capacitación y actualización** al personal del CERT-PY • **Recursos** técnicos y la infraestructura del CERT-PY.
CAPACIDAD DE INVESTIGACIÓN Y PERSECUCIÓN DE LA CIBERDELINCUENCIA	• **Programa de capacitación** para las fuerzas del orden en delincuencia cibernética • **Programa de capacitación** a agencias de procuración de justicia y jueces • **Recursos técnicos** y en herramientas para la Policía • **Requisitos mínimos** y control de calidad para investigar delitos • **Reglamentaciones y proyectos de ley** para la persecución de delitos • **Sesiones de consulta** con redactores legislativos y otras partes interesadas • **Convenio de Budapest** y leyes adicionales • **Punto de contacto** para la Red 24/7 (denuncia) • **Mecanismos** para compartir información sobre delitos
ADMINISTRACIÓN PÚBLICA Y	• **Directrices** para la adquisición, desarrollo y gestión de productos y servicios TIC • **Ejercicio de precalificación** de productos y servicios TIC y proveedores de servicios • **Unidades especializadas** de TIC y ciberseguridad

EJES	PRODUCTOS ESPERADOS
COORDINACIÓN NACIONAL	• **Sistema Nacional** de Ciberseguridad • **Normativa y grupos de trabajo** temáticos • **Asociación de profesionales** de las TIC para difusión de alertas tempranas • **Guía de Buenas Prácticas** de TIC y de Ciberseguridad. • **Canales de comunicación** entre actores • **Convenios de colaboración y cooperación** entre el sector privado y el sector público • **Mecanismos** para compartir información con organismos internacionales

Fuente: Elaboración propia a partir de (SENATICs, 2017)

ANEXO 3

Cuadro 12. Lineamientos estratégicos, iniciativas y metas propuestas en el Plan Nacional TIC 2022 – 2030

EJES	INICIATIVAS	METAS
Capacidad de Gestión de Incidentes Cibernéticos	• Fortalecer el **CERT-PY.** • Crear un **SOC gubernamental.** • Crear un **centro de operaciones de ciberseguridad.** • Crear **cargos** dentro de cada una de las instituciones • Destinar **recursos necesarios** para contratar nuevos funcionarios y tercerizar.	• Responder el 100% de los incidentes reportados. • Resolver en no más de 48hs desde el reporte. • Visibilizar los eventos de seguridad cibernética en al menos el 50% de los OEE.
Sistema de Intercambio de Información de Ciberseguridad	• Adquirir **mecanismos y sistemas de TI.** • Formar **profesionales de TI.** • Generar **boletines y alertas** de manera oportuna. • Establecer un **modelo de negocio** para dimensionar el costo de los servicios. • Evaluar una posible asignación de una **partida presupuestal.**	• Contar con mecanismos de alerta temprana de amenazas, mediante diversos canales y formatos como boletines y alertas de alto nivel
Protección de Sistemas de Gobierno e Infraestructura Crítica	• Adquirir e implementar, de manera centralizada, **mecanismos de protección específicos** para sistemas de Gobierno. • Definir los criterios y parámetros para identificación de **Infraestructuras críticas y servicios esenciales.** • Crear, implantar, adoptar y monitorear un **marco normativo** de protección de infraestructuras críticas, servicios esenciales y servicios digitales.	• Contar con un Oficial de Seguridad de la Información responsable de la seguridad de la información en el 100% de los OEE, dedicado y calificado en Ciberseguridad.
Formación de Capacidades en Ciberseguridad y Concienciación	• Adelantar **campañas de sensibilización** con un enfoque específico en temas de Ciberseguridad. • Incluir Ciberseguridad en todos los niveles de enseñanza, desde el escolar básico hasta los niveles universitarios. • Crear un **programa permanente de capacitación** de jueces, fiscales, policías y demás actores del sistema de justicia. • Realizar **campañas nacionales e integrales de concienciación** en materia de Ciberseguridad para diversos públicos objetivos.	• Aumentar el 50% de la cantidad de personas capacitadas y/o certificadas en Ciberseguridad a nivel técnico y profesional.

Fuente: Elaboración propia a partir de (MITIC, 2022)

ANEXO 4

La Agenda Digital es el Plan de Acción de la Estrategia de Transformación Digital del Paraguay y es la hoja de ruta que busca el aprovechamiento de las Tecnologías de Información y Comunicación (TIC) en la relación del Estado con la ciudadanía y las empresas, la economía digital, y el avance de la conectividad del Paraguay[32].

Actualmente se ejecuta un *Programa de Apoyo a la Agenda Digital* con el fin de apoyar las transformaciones sustanciales sobre cuatro componentes estratégicos: i) *Gobierno Digital,* ii) *Economía Digital*; iii) *Conectividad Digital,* y iv) *Fortalecimiento Institucional*. Bajo el componente *Gobierno Digital*, se estableció el producto "*Sistema Nacional de Ciberseguridad*" en donde se pretende la mejora de la capacidad de gestión de incidentes cibernéticos a través del CERT-PY y el Security Operations Center (SOC) gubernamental, y la creación de un sistema de intercambio de información de ciberseguridad con boletines informativos.

Bajo este producto también se incluye: i) Revisión del marco regulatorio, ii) Manejo de incidentes e investigaciones a través del SOC, iii) Implementación de un equipo de seguridad para infraestructuras críticas, iv) Creación de capacidad en ciberseguridad a nivel nacional, v) Investigaciones de análisis forense (remotas o in situ), y vi) Soluciones y productos de seguridad para las instituciones públicas, empresas y/o ciudadanos (solución de autenticación de doble factor centralizada para instituciones públicas, plugin antibotnet, otros).

Cuadro 13. Bienes adquiridos y Servicios contratados en el marco del Programa de Apoyo de la Agenda Digital para fortalecer el Sistema Nacional de Ciberseguridad

Año	Bienes adquiridos y Servicios contratados
2024	Servicio de monitoreo y elaboración de boletines y alertas de ciberseguridad Implementación de la metodología DevSecOps en MITIC Diagnósticos y auditorías de seguridad a instituciones públicas Asistencia Técnica de Seguridad a Instituciones Públicas Análisis y gestión de vulnerabilidades de sistemas de software Adquisición de Equipos, Instalación, Configuración y Servicios Conexos para el Proyecto de SOC
2023	Servicio de monitoreo y elaboración de boletines y alertas de ciberseguridad Implementación de la metodología DevSecOps en MITIC Diagnósticos y auditorías de seguridad a instituciones públicas Asistencia Técnica de Seguridad a Instituciones Públicas Análisis y gestión de vulnerabilidades de sistemas de software
2022	Servicio de monitoreo y elaboración de boletines y alertas de ciberseguridad Implementación de la metodología DevSecOps en MITIC Diagnósticos y auditorías de seguridad a instituciones públicas Asistencia Técnica de Seguridad a Instituciones Públicas
2021	Servicio de monitoreo y elaboración de boletines y alertas de ciberseguridad

Fuente: https://mitic.gov.py/

[32] Teniendo en cuenta lo establecido en la Ley N° 6298/2019, esta Agenda Digital está financiada por el Contrato de Préstamo No. 4650/OC-PR firmado el 6 de diciembre de 2018 y suscrito entre la República del Paraguay, en cabeza del MITIC, y el Banco Interamericano de Desarrollo (BID), hasta por un monto de US$ 130 millones. A 30 de septiembre de 2024, se han comprometido US$ 42,3 millones y se han ejecutado US$ 32,8 millones (https://www.iadb.org/es/proyecto/PR-L1153).


www.mitic.gov.py
www.cert.gov.py