UNIVERSIDAD METROPOLITANA DE ASUNCIÓN
Rca. Dominicana 387, Asunción - Paraguay - Tel.: (+595) 21 203761 / 21 229399 / 981 65700 / 981 415626
uma@uma.edu.py / www.uma.edu.py / www.facebook.com/UMA.Paraguay

Asunción, 22 de mayo de 2025
UMA/REC/44/22/05/2025

HONORABLE CAMARA DE DIPUTADOS
DIRECCION DE MESA DE ENTRADA
FECHA DE RECEPCION
DIA 23 / MES 05 / AÑO 2025
HORA: 10:22
Rebeca Britos
RESPONSABLE

Don
Dip. Nac. German Solinger Santander, Presidente
Comisión de Ciencia y Tecnología
Honorable Cámara de Diputados - HCD
E. S. D.

De mi consideración:

Tengo el agrado de dirigirme a Ud. a fin de saludarle cordialmente y, por su digno intermedio, a los demás miembros de esta Honorable Cámara de Diputados. Así mismo, en esta oportunidad honrar el compromiso del Centro de Investigación y Análisis Estratégicos de la Universidad Metropolitana de Asunción (CIAE - UMA), a fin de entregar el Anteproyecto de Ley de Ciberseguridad para la República del Paraguay, el cual cumplo en depositar en Mesa de Entrada. Así también se hizo entrega de una copia del mencionado Anteproyecto de Ley al Diputado Nacional Don Raúl Latorre, Presidente de la Honorable Cámara de Diputados, teniendo en cuenta que ambos Declararon de Interés Nacional según **Declaración N° 688/2024 "Que declara de interés nacional, el evento Internacional Taller Estratégico de Ciberseguridad"**, llevado a cabo del 24 al 26 de setiembre de 2024, en la Universidad Metropolitana de Asunción, con el patrocinio de la Embajada de los Estados Unidos de América, la Oficina de Cooperación de Defensa de los EE. UU en Paraguay, el Centro de Estudios Hemisféricos de Defensa William J. Perry y el copatrocinio de la Universidad Metropolitana de Asunción.

Al agradecer su atención, hago propicia la ocasión para renovarle mi más distinguida consideración y estima, aguardando sus mejores oficios, en la certeza de su valoración efectiva ante tan esmerada labor cooperativa.

Atentamente,

MARIA LIZ CECILIA GARCIA FRASQUERI
Firmado digitalmente por MARIA LIZ CECILIA GARCIA FRASQUERI
Fecha: 2025.05.22 22:04:52 -03'00'

Prof. Dra. María Liz García de Arnold
Rectora
Universidad Metropolitana de Asunción
asistenterectoria@uma.edu.py
+595 (0981) 534 760
+595 (0982) 546 540

CENTRO DE INVESTIGACIÓN Y ANÁLISIS ESTRATÉGICO
DE LA
UNIVERSIDAD METROPOLITANA DE ASUNCIÓN

"CIAE UMA"

Exposición de Motivos del anteproyecto de Ley de Ciberseguridad en Paraguay

El anteproyecto de Ley que se presenta tiene como propósito fundamental establecer un Marco Normativo Integral que permita garantizar la seguridad, estabilidad y resiliencia del ciberespacio en la República del Paraguay. Este marco legal surge como una respuesta estratégica a las crecientes amenazas y desafíos que plantea la era digital, tanto a nivel nacional como internacional, y busca posicionar al país a la vanguardia de las políticas de Ciberseguridad, **proteger las Infraestructuras Criticas del País y garantizar la Soberanía Tecnológica y Digital del Paraguay.**

En el contexto actual, donde las tecnologías de la información y la comunicación (TIC) desempeñan un rol esencial en las actividades económicas, sociales y gubernamentales, **el ciberespacio se ha convertido en un dominio crítico para la seguridad nacional**. Sin embargo, también se presenta como un terreno altamente vulnerable a ciberataques, infracciones legales y amenazas que podrían comprometer las infraestructuras críticas, la soberanía, la privacidad de los ciudadanos y el desarrollo económico del país. La inexistencia de una **Ley específica en esta materia**, hasta la fecha, subraya la urgencia de adoptar medidas que permitan garantizar un **entorno tecnológico y digital seguro y confiable**.

Con este objetivo, el anteproyecto de ley establece disposiciones claras que consolidan una **estrategia nacional de ciberseguridad** orientada a proteger las infraestructuras críticas, desarrollar capacidades efectivas de prevención y respuesta ante incidentes cibernéticos, y fomentar la cooperación tanto nacional como internacional, con una gobernanza sólida que tendrá la capacidad y responsabilidad de diseñar, coordinar y supervisar la implementación de políticas públicas y estrategias. En razón a lo señalado, se prioriza la creación de un Vice Ministerio de Ciberseguridad, tendiente a futuro, a convertirse en un órgano autárquico de aplicación como ser una Agencia Nacional de Ciberseguridad (ANCI).

Así mismo, el anteproyecto de ley subraya la importancia de promover la **investigación, innovación tecnológica y educación en ciberseguridad**. Reconoce que la capacitación constante de los actores claves, el desarrollo de campañas de sensibilización y la incorporación de esta temática en los planes educativos a todos los niveles son elementos fundamentales para generar una cultura de seguridad digital. A través de estas acciones, se busca no solo mitigar los riesgos asociados a las amenazas cibernéticas, sino también fortalecer la confianza de los ciudadanos y las instituciones en el uso seguro de las tecnologías.

Este anteproyecto incorpora estándares internacionales y protocolos técnicos que permiten alinear las normativas nacionales con las mejores prácticas globales en Ciberseguridad. Este enfoque enfatiza la adhesión de Paraguay a Tratados Internacionales, como el Convenio de Budapest, y refuerza su presencia y representación en foros y Organismos Internacionales relacionados con la Seguridad Cibernética. La promoción de alianzas entre los sectores público y privado también ocupan un lugar destacado, con el objetivo de coordinar esfuerzos, recursos y conocimientos para enfrentar de manera conjunta los desafíos del mundo digital.

Finalmente, esta normativa establece mecanismos claros para la **prevención, detección y respuesta ante incidentes Cibernéticos**, incluyendo auditorías periódicas, certificaciones de cumplimiento. El anteproyecto de ley incluye disposiciones específicas para regular el tratamiento de datos, la protección de infraestructuras críticas y la tipificación de delitos cibernéticos, como el hacking, el fraude digital y el ciberterrorismo, contemplando sanciones proporcionales a la gravedad de los actos cometidos.

De esta manera, **este anteproyecto de ley representará un paso trascendental en la consolidación de un entorno digital seguro, resciliente e inclusivo, con Multidominio, adaptado a las necesidades y retos del siglo XXI**. Su promulgación como Ley, e implementación reflejarán el compromiso de la República del Paraguay, con la Seguridad, la Defensa y el Desarrollo, salvaguardando su soberanía digital y contribuyendo al fortalecimiento de la Paz y la estabilidad en el Ciberespacio Global.

UNIVERSIDAD METROPOLITANA DE ASUNCIÓN
UMA
LEY Nº 2073/03
RECTORADO

MARIA LIZ CECILIA GARCIA FRASQUERI

Firmado digitalmente por MARIA LIZ CECILIA GARCIA FRASQUERI
Fecha: 2025.05.22 20:35:16 -03'00'

ANTECEDENTES

- En el año 2017 el Gobierno Nacional establece la implementación del Plan Nacional de Ciberseguridad aprobado en el año 2015 por Decreto del Poder Ejecutivo N° 7052. En ese sentido, en julio de 2022, la Universidad Metropolitana de Asunción presenta a su comunidad educativa y, a la Sociedad Paraguaya, capacitaciones y seminarios conjuntos con el Centro de Estudios Hemisféricos de Defensa William J. Perry, mediante el convenio de cooperación vigente entre ambas instituciones.
- En el contexto señalado, en septiembre de 2024, el Centro de Investigación y Análisis Estratégico de la Universidad Metropolitana de Asunción (CIAE - UMA), con el patrocinio de la Embajada de los Estados Unidos de América, la Oficina de Cooperación de Defensa de los EE.UU en Paraguay, el Centro de Estudios Hemisféricos de Defensa W.J.P. y, el copatrocinio de la UMA, han liderado una serie de iniciativas estratégicas orientadas al fortalecimiento de las capacidades nacionales en Ciberseguridad.

Principales Iniciativas

1. **Seminario Internacional de Ciberseguridad;** Organizado con expertos del Centro de Estudios Hemisféricos de Defensa William J. Perry (W.J.P.), de la Universidad Nacional de la Defensa de los EE.UU., académicos investigadores, con el liderazgo del Director de Ciberseguridad de W.J.P. Gral. (r) Dr. Boris Saavedra, y la participación de expertos de los siguientes países: **Colombia, México, Perú, EE.UU** entre otros, incluida, la Prof. Ing. Dra. Angélica Castillo Rios (Peru) quien fuera galardonada con el prestigioso premio en materia de

Ciberseguridad, durante una ceremonia celebrada en el Castillo de Bled, Slovenia. (años 2023 y 2024)

Participantes:
Miembros de la Academia, de las Fuerzas Armadas, de la Policía Nacional, de los Poderes; Ejecutivo, Legislativo y Judicial, Entes Autárquicos, componentes de instituciones del Sector Público y Privado.

2. **Talleres Regionales de Ciberseguridad,** desarrollados en el Alto y Bajo Chaco Boreal, liderado por él Director de Ciberseguridad del C.W.J.P. Gral. (r) Dr. Boris Saavedra, y la participación de expertos nacionales en el área de Tecnología y Ciberseguridad. En estos talleres, se abordaron temas de Ciberseguridad y Geopolítica referente a la Geoeducación, Geociencias y Geoeconomía, teniendo como contenidos: Ciberdefensa, Infraestructura críticas, la relación de la ciencia espacial con la ciberseguridad, inteligencia artificial, entre otros.

En los eventos, participaron invitados de la Comunidad Educativa, de las Fuerzas Armadas, de la Policía Nacional, de la Sociedad Civil, entes Públicos y Privados, Autoridades Departamentales de los Departamentos de Boquerón y Villa Hayes.

3. **Ciclo de Conversatorios Académicos** dirigidos a Facultades de Ciencias Jurídicas y de Humanidades de la UMA, del Centro de Estudios Hemisféricos de Defensa, Capítulo Paraguay, del Instituto de Altos Estudios Estratégicos (IAEE), del Ministerio de Tecnología de la Información y la Comunicación (MITIC), de la Dirección General de TIC's de las Fuerzas Militares, del Instituto Superior de Educación Policial, del Comando de Institutos Aeronáuticos de Enseñanza, del Ministerio de Defensa.
4. **El Convenio de Cooperación** suscripto con el Ministerio de la Defensa Pública y la Universidad Metropolitana de Asunción ha permitido contar con el concurso de abogados-académicos, Defensores Públicos que aportaron en el documento, la

perspectiva técnico-jurídica en lo concerniente a la elaboración de este Anteproyecto de Ley de Ciberseguridad.

5. Síntesis: Repercusiones en la Prensa y Redes

A. Declaraciones Institucionales y Políticas

Durante la cobertura del evento, se destacó la preocupación de las Autoridades Paraguayas por la creciente vulnerabilidad del país en el Ciberespacio.

Puntos más relevantes:

- **Crimen organizado, terrorismo y ciberseguridad** fueron identificados como áreas críticas que requieren una **readecuación urgente** en la gestión estatal y militar.
- Se reconoció la **fragilidad del país en materia de seguridad digital**, tanto en infraestructura como en legislación.

El **Presidente de la Cámara de Diputados, Honorable Dip Dr. Raul Latorre** enfatizó que la seguridad es una **responsabilidad ineludible del Estado**, y subrayó la necesidad de fortalecer las capacidades de **militares, fiscales y servidores públicos**.

- En el evento se valoró positivamente la **presencia de los Honorables Miembros del Congreso Nacional:** Sen. Patrick Kemper, Sen. Lilian Samaniego, Sen. Eduardo Nakayama, Sen. Jose Oviedo, Dip. Raul Latorre, Dip. Pedro Ortiz, Dip. German Solinger, Dip. Rocio Vallejos, lo que augura una **respuesta legislativa conjunta** a los desafíos en Ciberseguridad.
- Se agradeció la colaboración de **delegaciones extranjeras**, destacando su aporte en el fortalecimiento de capacidades nacionales.

B. Comunicación de la Embajada de EE.UU.

La **Embajada de los Estados Unidos en Paraguay**, a través de su cuenta oficial en redes sociales, comunicó:

"Ha culminado con éxito el Taller Estratégico de Ciberseguridad, llevado a cabo por expertos internacionales del @WJPerryCenter, a través de nuestra Oficina de Cooperación de Defensa y en colaboración con la @UMA. Un entorno colaborativo, centrado en temas de ciberseguridad, que contó con la participación de representantes del gobierno, del sector financiero y de la academia."

Este mensaje refuerza el carácter **multisectorial y colaborativo** del evento, así como el compromiso de EE.UU. con el fortalecimiento de la ciberseguridad en Paraguay.

C. Conclusiones Claves

- Necesidad urgente de una **Ley de Ciberseguridad integral**, basada en estándares internacionales, aplicabilidad y sostenibilidad.
- Relevancia de una **Gobernanza Estratégica**, fortalecimiento institucional y formación continua.
- Propuesta de mantener la participación activa de los asistentes en la revisión del anteproyecto de ley y en futuras capacitaciones.
- Visión compartida para construir un **Ecosistema Digital seguro, confiable y resiliente**, que posicione a la Ciberseguridad como un pilar del Desarrollo Nacional.

UNIVERSIDAD METROPOLITANA DE ASUNCION UMA LEY Nº 2073/03 RECTORADO

Estas acciones, asumidas con alto compromiso académico y patriótico, permitieron al CIAE - UMA consolidar un proceso de investigación y análisis comparado de legislaciones internacionales, tratados y convenios ratificados por el Paraguay, concordantes con la normativa nacional vigente. Como resultado de este esfuerzo sostenido, plural, local e internacional, se ha culminado la redacción del presente **Anteproyecto de Ley de Ciberseguridad para la República del Paraguay**, acompañado de su respectivo **glosario técnico**.

Este documento se presenta ante la Honorable Cámara de Diputados como una contribución académica y estratégica, con el objetivo de contar con un Marco Normativo Nacional en materia de **Ciberseguridad**, proteger **las Infraestructuras Criticas del País y garantizar la Soberanía Tecnológica y Digital del Paraguay.**

MARIA LIZ CECILIA GARCIA FRASQUERI

Firmado digitalmente por MARIA LIZ CECILIA GARCIA FRASQUERI
Fecha: 2025.05.22 20:33:36 -03'00'

UNIVERSIDAD METROPOLITANA DE ASUNCIÓN
UMA
LEY Nº 2073/03
RECTORADO

Prof. Dra. María Liz García de Arnold
Rectora
Universidad Metropolitana de Asunción
Presidente C.I.A.E UMA
asistenterectoria@uma.edu.py
+595 (0981) 534 760
+595 (0982) 546 540

LEY N° _____/2025

QUE CREA LA "LEY DE CIBERSEGURIDAD DE LA REPÚBLICA DEL PARAGUAY."

El Congreso de la Nación Paraguaya sanciona con fuerza de Ley:

Artículo 1. Objeto de la Ley

La presente ley tiene por objeto establecer el marco legal en el ámbito de la ciberseguridad dentro de la República del Paraguay conteniendo principios, mecanismos, y aspectos regulatorios para garantizar el entorno de la ciberseguridad dentro del dominio del Estado Paraguayo y, proteger las infraestructuras críticas, la información y sus sistemas, así como los derechos de las personas frente a amenazas y hechos punibles cibernéticos.

El Estado Paraguayo establece como su soberanía el dominio paraguayo en el Ciberespacio. Esto incluye capacidades multimedia de amenaza hibrida, en la adopción de medidas de prevención y mitigación relacionado a la ciberseguridad, fortalecer la resiliencia social y la comunicación estratégica Interdependiente, incluyendo la Inteligencia Artificial (IA) y la regulación de las redes sociales sobre bases de la territorialidad.

Artículo 2. Ámbito de Aplicación

La presente ley se aplica a todas las personas físicas y jurídicas, incluyendo a la academia, entidades, operadores y prestadores de servicios digitales, públicas y privadas. Así como a ciudadanos y residentes temporales que interactúen o utilicen sistemas y activos cibernéticos en el ciberespacio dentro del territorio nacional, así como a las infraestructuras críticas identificadas conforme a esta normativa.

Artículo 3. Glosario

A los efectos de esta ley, se entenderán por:

a) **AMENAZAS EN MÚLTIPLES DOMINIOS:** La nueva doctrina de Operaciones Multidominio (MDO) plantea contrarrestar amenazas simultaneas en todos los dominios de la guerra mediante la convergencia de efectos y fuerzas.
b) **ANÁLISIS SITUACIONAL Y PROSPECTIVO:** Evaluación continua de riesgos, vulnerabilidades y tendencias en el ciberespacio realizada por el CNRIC, para anticipar amenazas y fortalecer la prevención y respuesta nacional.
c) **ARANCELES:** Los aranceles son impuestos o tarifas que un país cobra a los productos importados o exportados. Su objetivo principal es regular el comercio internacional y proteger la economía local.
d) **CIBERAMENAZAS:** son riesgos o peligros que pueden comprometer la seguridad de sistemas informáticos, redes, datos y servicios digitales en el ciberespacio. Estas amenazas pueden ser activas o potenciales, y abarcan una amplia gama de ataques, actividades maliciosas o vulnerabilidades explotables que buscan causar daño, robo, interrupción o acceso no autorizado. (Virus y malware – Phishing – Ransomware - Ataques a infraestructuras críticas - Espionaje cibernético)
e) **CIBERATAQUES:** Son acciones malintencionadas llevadas a cabo en el ciberespacio con el objetivo de dañar, interrumpir, acceder ilegalmente o

comprometer sistemas informáticos, redes, datos o servicios digitales. **(Phishing –Ransomware - Ataque DDoS (Denial of Service Distribuido - Inyección SQL – Malware)**

f) **CIBERCRIMEN: (o delito informático)** se refiere a cualquier actividad ilegal que se lleva a cabo utilizando computadoras, redes o dispositivos digitales. Estos delitos pueden tener como objetivo sistemas informáticos, datos personales, financieros o incluso infraestructuras críticas.

g) **CIBERDEFENSA:** La Ciberdefensa se refiere al conjunto de estrategias, políticas, acciones y medidas técnicas diseñadas para proteger sistemas informáticos, redes, datos y servicios digitales frente a amenazas y ataques cibernéticos. Su objetivo principal es garantizar la seguridad nacional y soberanía digital en cuanto la protección de infraestructuras críticas, y la resiliencia de los entornos digitales, tanto en el ámbito personal, empresarial como gubernamental

h) **CIBERDELITOS**: se refiere a delitos tipificados en el código penal de un país, cometidos a través de medios digitales, como puede incluir tanto delitos informáticos como delitos tradicionales adaptados al entorno digital: Estafas por internet - Suplantación de identidad – Ciberacoso – Grooming - Ejemplo: Una persona que crea un perfil falso en redes sociales para acosar a otra.

i) **CIBERESPACIO:** Es el espacio donde se desarrollan actividades relacionadas con el uso de internet, redes de comunicación y sistemas electrónicos. (globalidad – virtualidad - Interactividad)

j) **CIBERTERRORISMO:** Es el uso del ciberespacio y las tecnologías digitales y virtuales para llevar a cabo actos terroristas. Estos actos tienen como objetivo causar daño significativo, crear miedo en la sociedad, desestabilizar sistemas, o promover una agenda ideológica, política o religiosa mediante ataques cibernéticos.

k) **CIBERSEGURIDAD:** Conjunto de medidas, herramientas y acciones destinadas a proteger los sistemas, redes y datos digitales contra accesos no autorizados o ataques.

l) **CONCIBER.** Consejo Nacional de Ciberseguridad.

m) **DOMINIO EN DEFENSA Y SEGURIDAD**: El dominio en defensa y seguridad se refiere a una esfera o medio especifico en el que se llevan a cabo actividades militares o de seguridad para alcanzar objetivos.

n) **E-CIBER PARAGUAY:** Estrategia Nacional de Ciberseguridad

o) **FONTIC:** Fondo Nacional de Tecnologías de la Información y Comunicación

p) **HOMOLOGACION:** proceso de validación y certificación mediante el cual una institución (pública o privada) verifica equipos y sistemas si cumplen con ciertos requisitos técnicos, funcionales, legales o de seguridad antes de ser aprobado para su uso local y comercialización.

q) **INCIDENTE CIBERNÉTICO:** Evento que comprometa la integridad, confidencialidad o disponibilidad de información o sistemas digitales.

r) **INFRAESTRUCTURA CRÍTICA:** Sistemas físicos, digitales o virtuales esenciales para la seguridad nacional, la economía o el bienestar social, incluyen servicios como telecomunicaciones, energía, agua, transporte, servicios de emergencia.

s) **INTELIGENCIA ARTIFICIAL GENERATIVA (IAG):** Es un tipo de inteligencia artificial que utiliza modelos avanzados de aprendizaje automático, para generar contenido nuevo y original a partir de datos existentes. Esta tecnología tiene la capacidad de crear texto, imágenes, audio, videos, y otros tipos de

datos en respuesta a ciertas instrucciones o condiciones definidas por los usuarios.

t) **MITIC:** Ministerio de Tecnologías de la Información y Comunicación
u) **NANOTECNOLOGIA:** Es la disciplina que se encarga de la manipulación de la materia a escala nanométrica (una mil millonésima parte del metro) con el fin de crear materiales, dispositivos y sistemas con nuevas propiedades y aplicaciones.
v) **NOTIFICACIÓN DE INCIDENTES:** Reporte obligatorio de incidentes cibernéticos dentro de 24 horas, indicando el impacto y características del evento.
w) **RESILIENCIA:** Capacidad de continuar Operando bajo situaciones adversas con eficiencia y eficacia.
x) **TASAS:** pago obligatorio que se hace al Estado o a una entidad pública a cambio de un servicio específico.

Artículo 4. Créase la Estrategia Nacional de Ciberseguridad (E-Ciber Paraguay).

El E-Ciber Paraguay definirá las políticas, objetivos, acciones y directrices para garantizar y fortalecer la seguridad y protección del ciberespacio paraguayo, a ser elaborado y actualizado periódicamente por el MITIC a través del Vice Ministerio de Ciberseguridad. El Poder Ejecutivo diseñará y aplicará esta estrategia con la participación de los sectores público, privado y la academia.

Artículo 5. Estructura Orgánica del MITIC

El Ministerio contará con la siguiente estructura orgánica:

a) Ministro;
b) Dirección General de Gabinete Ministerial;
c) Secretaria General;
d) Viceministerio de Tecnologías de la Información y Comunicación (TIC);
e) Viceministerio de Comunicación
f) Viceministerio de Ciberseguridad
g) Dirección General de Asesoría Jurídica;
h) Dirección General de Administración y Finanzas;
i) Auditoría Interna; y,
j) Otras Direcciones Generales y dependencias que fueren necesarias para el cumplimiento de los objetivos del Ministerio.

En caso de sustitución del Ministro, los cargos de los titulares de las unidades orgánicas detalladas en el presente artículo, estarán a disposición de la nueva autoridad designada por el Poder Ejecutivo, pudiendo ser reasignados según necesidad o destituidos sin más trámites por término de funciones.

Artículo 6º. Estructura del Viceministerio de Ciberseguridad

Se crea el Viceministerio de Ciberseguridad, dependiente del Ministerio de Tecnologías de la Información y Comunicación (MITIC), con funciones específicas para la implementación de esta ley.

1. **Viceministerio de Ciberseguridad:**

a) Dirección General de Incidentes CERT PY
c) Dirección General de Políticas y Homologaciones.

Artículo 7. Competencias del Viceministerio de Ciberseguridad

a) Dirigir y coordinar la ejecución de la Estrategia Nacional de Ciberseguridad (E-Ciber Paraguay) en todos los niveles del sector público y privado.

b) Supervisar y evaluar el desempeño de las Instituciones del Estado en la implementación de la presente ley, garantizando su operatividad y eficacia.

c) Gestionar los recursos humanos, técnicos y financieros asignados a la ciberseguridad, optimizando su uso para el cumplimiento de las políticas nacionales.

d) Proponer directrices vinculantes para las entidades sujetas a esta ley.

e) Informar periódicamente al CONCIBER y a la ciudadanía, sobre el estado de la ciberseguridad en el país, presentando reportes anuales y propuestas de mejoras, preservando el cumplimiento de la ley de transparencia.

f) Diseñar, y actualizar la Estrategia Nacional de Ciberseguridad (E-Ciber Paraguay), definiendo objetivos, prioridades y plazos para su cumplimiento en el ámbito público y privado.

g) Coordinar acciones entre instituciones públicas, el sector privado y organismos internacionales para garantizar una respuesta unificada ante amenazas cibernéticas.

h) Supervisar el cumplimiento de las disposiciones de esta ley por parte de las entidades sujetas a su ámbito, incluyendo operadores de infraestructuras críticas y prestadores de servicios esenciales.

i) Promover la investigación, desarrollo e innovación en tecnologías de ciberseguridad, fomentando alianzas con centros académicos y tecnológicos.

j) Representar a Paraguay en foros y acuerdos internacionales relacionados con la ciberseguridad, asegurando la alineación con estándares globales.

Artículo 8. Consejo Nacional de Ciberseguridad (CONCIBER)

Crease el Consejo Nacional de Ciberseguridad (CONCIBER) que estará integrado por representantes de:

a- Un representante titular y suplente nombrado por el Poder Ejecutivo, cuya titularidad ejercerá el Ministro del MITIC y como suplente el Vice Ministro de Ciberseguridad, sobre quienes recaerá la Presidencia del CONCIBER.
b- Un representante titular y suplente del Poder Legislativo
c- Un representante titular y suplente del Poder Judicial
d- Un representante titular y suplente del Ministerio Publico
e- Un representante titular y suplente de las Fuerzas Militares
f- Un representante titular y suplente del Ministerio del interior
g- Un representante titular y suplente de ANDE (Administración Nacional de Electricidad)

h- Un representante titular y suplente de licenciatarios de servicio de internet fijo
i- Un representante titular y suplente de Universidades Privadas
j- Un representante titular y suplente del Centro Nacional de Computación UNA
k- El Ministro Secretario o Viceministro de la Secretaria Nacional de Inteligencia dependiente de la Presidencia de la Republica.

Los miembros del CONCIBER contemplados en los incisos (g), (h), (i), (j) serán nombrados por el Presidente de la Republica de acuerdo a postulaciones recibidas por parte de los gremios vinculantes ante la convocatoria realizada. En caso de que no existan nominados, el Presidente de la Republica nombrará directamente a los miembros que integrarán este Consejo. Los Miembros del CONCIBER durarán cinco años en sus funciones, pudiendo ser reelectos por un período más y no percibirán haberes adicionales más los percibidos por parte de sus Instituciones o Empresas.

Artículo 9. Funciones del CONCIBER:

a. Asesorar al MITIC a través del Viceministerio de Ciberseguridad en propuestas de formulación de políticas y estrategias nacionales e internacionales de ciberseguridad, aportando perspectivas multisectoriales.
b. Proponer medidas preventivas y de respuesta ante amenazas cibernéticas, basadas en análisis de riesgos y tendencias identificadas.
c. Evaluar la efectividad de las políticas públicas vigentes y la implementación de sus estrategias, emitiendo recomendaciones periódicas cuando las condiciones requieran.
d. Facilitar la cooperación entre el sector público, privado y la academia, promoviendo la participación activa de empresas y organizaciones en la materia pertinente.
e. Proponer planes de contingencia nacionales para incidentes cibernéticos de gran escala.
f. Asesorar al Viceministerio de Ciberseguridad en propuestas de formulación de políticas y estrategias nacionales e internacionales de ciberseguridad, aportando perspectivas multisectoriales.
g. Proponer medidas preventivas y de respuesta ante amenazas cibernéticas, basadas en análisis de riesgos y tendencias identificadas por el CONCIBER.
h. Evaluar la efectividad de las políticas publica vigentes y la implementación de sus estrategias, emitiendo recomendaciones periódicas cuando las condiciones requieran.
i. Facilitar la cooperación entre el sector público, privado y la academia, promoviendo la participación activa de empresas y organizaciones en la materia pertinente.
j. Aprobar planes de contingencia nacionales para incidentes cibernéticos de gran escala, en coordinación con el CONCIBER.

Artículo 10.- Absorción del Fondo Nacional de Tecnologías de la Información (FONTIC). Componentes.

El Ministerio absorbe como parte de sus recursos económicos, el (FONTED), el cual pasara a llamarse Fondo Nacional de Tecnologías de la Información y Comunicación

(FONTIC), constituido con la finalidad de lograr los objetivos vinculados con programas de Tecnologías de la Información y Comunicación (TIC).

Forman parte del Fondo Nacional de Tecnologías de la Información y Comunicación (FONTIC):

1.Los fondos provenientes de convenios o acuerdos con instituciones nacionales o internacionales, públicas o privadas que se enmarquen en programas relacionados con las Tecnologías de la Información y Comunicación (TIC).
2. Los recursos provenientes de la cooperación técnica internacional, que se enmarquen en programas relacionados con las Tecnologías de la Información y Comunicación (TIC).
3. El 50 % (cincuenta por ciento)) de los recursos afectados al Fondo de Servicios Universales, administrado por la Comisión Nacional de Telecomunicaciones (CONATEL).
4. Los recursos provenientes de los Royalties y Compensaciones que corresponden a la Administración Central, de conformidad a lo establecido en el inciso a) del Artículo 1º de la Ley Nº 3984/2010, "QUE ESTABLECE LA DISTRIBUCION Y DEPOSITO DE PARTE DE LOS DENOMINADOS "ROYALTIES" Y "COMPENSACIONES EN RAZON DEL TERRITORIO INUNDADO A LOS GOBIERNOS DEPARTAMENTALES Y MUNICIPALES ", en un monto que deberá establecerse en cada Ejercicio Fiscal.
5. Los aranceles y tasas por homologaciones de equipos, accesorios y demás componentes de orden informático, así como softwares de ciberseguridad; importados y comercializados dentro del territorio nacional por personas físicas y jurídicas de orden público o privado que serán destinados a financiamiento de planes y programas de Ciberseguridad.
6. Además, podrán formar parte de los recursos del Fondo Nacional de Tecnologías de la Información y Comunicación (FONTIC) las donaciones, legados, transferencias u otros aportes, por cualquier título proveniente de personas naturales o jurídicas nacionales o extranjeras, que se enmarquen en programas relacionados con las Tecnologías de la Información y Comunicación TIC.

Artículo 11. De las Infraestructuras Críticas

Los operadores de infraestructuras críticas deberán cumplir con los protocolos de seguridad y prevención establecidos por el MITIC para proteger sus sistemas y prevenir incidentes cibernéticos. A tal efecto, estarán obligados a:

a) Aplicar medidas de seguridad obligatorias, conforme a los estándares y lineamientos definidos, que incluyan la gestión de riesgos, la actualización de sistemas y planes de respuesta a incidentes.

b) Notificar y reportar al MITIC ante cualquier incidente de acuerdo sus niveles de riesgos en un plazo máximo de 24 horas desde su detección, proporcionando un informe inicial que detalle la naturaleza y el impacto del evento.

Articulo 12. Cumplimiento Obligatorio

Los operadores y prestadores de servicios de telecomunicaciones afectados por la presente ley, instituciones públicas y privadas deberán adoptar medidas de protección y reportar incidentes cibernéticos conforme a los procedimientos establecidos. Estas medidas incluirán la gestión de riesgos, la actualización de sistemas y la elaboración de planes de respuesta a incidentes, con el objetivo de garantizar la continuidad y seguridad de los servicios. El incumplimiento de estas medidas y obligaciones será sancionado conforme a lo dispuesto en la presente ley.

Articulo 13. De las Notificaciones Obligatorias y Gestión de Incidencias

Toda entidad pública o privada sujeta a esta ley, incluyendo operadores de infraestructuras críticas y servicios esenciales, deberá notificar al MITIC cualquier incidente cibernético significativo dentro de las 24 horas desde su detección, proporcionando información inicial sobre la naturaleza y el impacto del evento. El MITIC de forma inmediata a través de sus dependencias vinculantes coordinará la gestión de incidencias y podrá requerir reportes adicionales dentro de plazos establecidos por reglamentación, especialmente en casos de incidentes graves que afecten la seguridad nacional o servicios esenciales.

Artículo 14. Identificación de Tipos de Ataques y Delitos Cibernéticos

El MITIC, a través del Viceministerio de Ciberseguridad, será el encargado de la identificación de los ataques cibernéticos, **debiendo comunicar al Ministerio Publico para su persecución penal**, cuando corresponda.

Dicha identificación incluirá, entre otros, el acceso ilegal a sistemas informáticos, el fraude cibernético, los ataques de ransomware, la denegación de servicio (DDoS) y otras amenazas significativas. Se detallarán sus características técnicas y sus potenciales impactos, y su relación acorde con hechos punibles tipificados **en el Código Penal vigente.**

Artículo 15. Homologación de equipos, accesorios y otros de orden informático

Están sujetas a la inspección, homologación, y supervisión que determine el MITIC a los equipos, softwares de ciberseguridad, accesorios, otros de orden informáticos-tecnológicos, incluida la nanotecnología, importados y comercializados dentro del territorio nacional, con el objeto de contar con registros y garantías de los mismos. Las personas físicas o jurídicas deberán contar autorizaciones o licencias de homologación por parte del MITIC previa comercialización.

Artículo 16. Incorporación de la Ciberseguridad en Planes Educativos

El Viceministerio de Ciberseguridad en coordinación con el Ministerio de Educación y Ciencias (MEC) promoverá y garantizará la incorporación de contenidos de ciberseguridad en los programas educativos de los niveles primario, secundario y universitario, tanto en instituciones públicas como privadas. Estos contenidos abarcarán conocimientos básicos sobre protección de datos, uso seguro de tecnologías y prevención de delitos cibernéticos, adaptados a cada nivel educativo. El

MEC elaborará, en un plazo no mayor a un año desde la promulgación de esta ley, una guía curricular específica en colaboración con expertos en ciberseguridad.

Artículo 17. Fomento de la Formación, Investigación y Concienciación en Ciberseguridad

El Viceministerio de Ciberseguridad, fomentará la formación, capacitación, investigación y concienciación en buenas prácticas de ciberseguridad. Para ello:

Implementará programas de capacitación dirigidos a la ciudadanía, empresas y organizaciones.

Promoverá investigaciones académicas y tecnológicas en alianza con universidades y centros especializados.

Ejecutará campañas anuales de concienciación sobre el uso seguro de tecnologías y la prevención de riesgos cibernéticos.

Artículo 18. Capacitación Obligatoria en Ciberseguridad

Los funcionarios públicos y los empleados de sectores estratégicos, incluyendo aquellos relacionados con infraestructuras críticas (salud, energía, transporte, comunicaciones y finanzas), recibirán formación obligatoria anual en ciberseguridad.

Esta capacitación será coordinada por el Viceministerio de Ciberseguridad, en conjunto con las instituciones correspondientes, y abarcará temas como prevención de ataques cibernéticos, manejo seguro de datos y respuesta a incidentes. El incumplimiento de esta obligación será considerado una falta administrativa sancionable conforme a la normativa vigente.

Artículo 19. Convenios de Cooperación Interinstitucional, Local e Internacional

Cooperación Internacional. El Estado paraguayo promoverá la cooperación en materia de ciberseguridad con organismos internacionales, países aliados y otras entidades relevantes, en línea con los principios establecidos en tratados internacionales como el Convenio de Budapest sobre Ciberdelincuencia. Para ello, impulsará la adopción de estándares internacionales reconocidos y fomentará la suscripción y cumplimiento de dichos tratados.

Cooperación Local e Interinstitucional. El Estado incentivará la celebración de acuerdos entre instituciones públicas, privadas y organizaciones locales para fortalecer la ciberseguridad nacional, promoviendo el intercambio de conocimientos, recursos y buenas prácticas.

Artículo 20. Adhesión a Tratados Internacionales

El Paraguay se compromete **a adoptar e implementar Convenio sobre Ciberdelincuencia y otros tratados internacionales pertinentes** en materia de ciberseguridad, ajustando su legislación y políticas nacionales para garantizar su efectiva aplicación. El estado evaluará periódicamente la pertinencia de adherirse a nuevos instrumentos internacionales que fortalezcan la lucha contra el Cibercrimen y **otros hechos punibles conexos.**

Artículo 21. Participación en Organismos Internacionales y Eventos de Ciberseguridad

El MITIC será la entidad encargada de representar al Paraguay en organismos internacionales, foros, conferencias y eventos relacionados con la ciberseguridad. Dicha representación incluirá la promoción de los intereses nacionales, el intercambio de experiencias y la colaboración en iniciativas globales para la protección del ciberespacio.

Artículo 22. Revisión, Actualización y Adopción de Estándares Internacionales

El Estado, a través del MITIC y en coordinación con otras instituciones competentes, revisará y actualizará periódicamente las políticas, normativas y estándares nacionales de ciberseguridad, alineándolos con las mejores prácticas y estándares internacionales. Asimismo, se adoptarán medidas para garantizar su implementación efectiva en todos los niveles del sector público y privado.

Artículo 23. Tipología de las Sanciones

a) **Procedimientos**: Se establecerán procesos sumarios administrativos y, eventuales sanciones, conforme al reglamento ajustado a las normas legales vigentes. Estos procedimientos garantizarán la preservación de pruebas digitales, la celeridad en la actuación y la cooperación con entidades nacionales e internacionales, especialmente en casos que involucren datos sensibles, servicios esenciales o infraestructuras críticas.
b) **Tipos de sanciones:** Las infracciones a la presente ley incluirán sanciones como ser; apercibimiento, multas, inhabilitación, para importadores, comerciantes, usuarios de sistemas informáticos y otros, según el nivel de la gravedad de la infracción, pudiéndose ser aplicadas en forma unitaria o múltiple, las sanciones administrativas por comisión de infracciones, en tales serian acumulativa y progresivamente, de acuerdo a la gravedad o reincidencia. Es decir, se podrá aplicar solamente el apercibimiento como sanción más leve, primeramente, a título de ejemplo, y luego un 2° apercibimiento como sanción y multa, hasta la más grave, la inhabilitación, sin perjuicio de otra multa, ya de monto mayor, (progresividad y acumulabilidad).
   En el caso de reincidencia de un infractor, se establece ya la cláusula de que sería "inaplicable el apercibimiento".

Artículo 24. Derogaciones y modificaciones normativas

Quedan derogadas las disposiciones contrarias a esta ley y modificada la Ley 6207/2018 en sus artículos 11, 12 y 18 que Crea el Ministerio de Tecnologías de la Información y Comunicación (MITIC).

Artículo 25. Disposiciones Transitorias

En un plazo no mayor a 180 (ciento ochenta días) el Ministerio de Tecnologías de la Información y Comunicación (MITIC) deberá readecuar todos los planes, programas y, proyectos enmarcados en Ciberseguridad, acorde a la presente Ley.

Artículo 26. El Poder Ejecutivo, reglamentará la presente Ley.
Artículo 27. Comuníquese al Poder Ejecutivo.

UNIVERSIDAD METROPOLITANA DE ASUNCIÓN UMA LEY Nº 2073/03 RECTORADO

MARIA LIZ CECILIA GARCIA FRASQUERI

Firmado digitalmente por MARIA LIZ CECILIA GARCIA FRASQUERI
Fecha: 2025.05.22 20:34:30 -03'00'