CONGRESO DE LA REPÚBLICA

COMISION DE ASUNTOS DE SEGURIDAD NACIONAL

26 de agosto de 2025

CONGRESO DE LA REPÚBLICA
DIRECCIÓN LEGISLATIVA
RECIBIDO
26 AGO 2025
FIRMA: HORA

Magister
Luis Eduardo López Ramos
Encargado de Despacho
Dirección Legislativa
Su Despacho

Estimado Luis Eduardo:

Con un atento y respetuoso saludo me dirijo a usted con el objeto de saludarlo, deseándole éxitos al frente de sus funciones.

Conforme a lo establecido en los Artículos 39, 40 y 41 de la Ley Orgánica del Congreso de la República, remito en forma física y digital el DICTAMEN FAVORABLE CON MODIFICACIONES, elaborado por la Comisión de Asuntos de Seguridad Nacional sobre la Iniciativa de Ley No. 6347 que dispone aprobar la Ley de Ciberseguridad, para su trámite correspondiente.

Sin otro particular y agradeciéndole su atención al presente, me suscribo con muestras consideración y estima.

Atentamente,

CONGRESO DE LA REPÚBLICA
COMISIÓN DE ASUNTOS DE SEGURIDAD NACIONAL
GUATEMALA, C. A.

Diputado Jorge Mario Villagrán Álvarez
Presidente

JMVA/mdep
Cc: file

CONGRESO DE LA REPÚBLICA

COMISIÓN DE ASUNTOS DE SEGURIDAD NACIONAL

DICTAMEN 01-2025
COMISIÓN DE SEGURIDAD NACIONAL
CONGRESO DE LA REPÚBLICA DE GUATEMALA

INICIATIVA 6347
INICIATIVA QUE DISPONE APROBAR
LEY DE CIBERSEGURIDAD

Honorable Pleno:

Con fecha 27 de febrero de 2024, fue presentada la iniciativa de ley por los diputados: 1. José Pablo Mendoza Franco; 2. Cristian Rodolfo Álvarez y Álvarez; y, 3. Gustavo Adolfo Cruz Montoya. La iniciativa fue identificada por la Dirección Legislativa con el número 6347 y dispone aprobar la Ley de Ciberseguridad, para su estudio, análisis y dictamen correspondiente.

I. ANTECEDENTES

La exposición de motivos de la iniciativa de ley menciona argumentos como:

La acelerada transformación digital de nuestras economías y sociedades aportan notables beneficios a empresas, organizaciones del sector público y particulares, desde una mayor competitividad y bienestar hasta una mayor resiliencia ante grandes catástrofes como la pandemia de COVID-19. Sin embargo, esta transformación ha incrementado la dependencia digital, así como el alcance, la escala y la complejidad general de los sistemas de información, redes, activos y flujos de datos de las organizaciones.

Los productos y servicios digitales no son lo suficientemente seguros y exponen a los usuarios a riesgos de seguridad, sin proporcionarles la información adecuada, ni los medios para mitigarlos. Las ciberamenazas continúan evolucionando debido a la facilidad de acceso, bajo costo, alta rentabilidad y el crecimiento exponencial de las inteligencias artificiales, por medio del uso de las plataformas digitales para fines delictivos.

Los métodos y sistemas de las tecnologías han evolucionado durante el tiempo; no obstante, la protección y control en los sistemas no van al mismo ritmo en dichos avances; por lo que, la falta de herramientas informáticas y conocimientos técnicos, son aprovechados por ciberdelincuentes quienes se encuentran innovando y sofisticando sus ataques, cada vez con mayor impacto. Por lo tanto, es necesario que las sociedades, a través de sus gobiernos, generen marcos legales que coadyuven a ejercer soberanía en el ciberespacio.

En Guatemala los ataques conocidos han sido los siguientes:

1. **Ataque al Ministerio de Finanzas Públicas (MINFIN) – Noviembre 2023**

   El 26 de noviembre de 2023, el MINFIN sufrió un ataque cibernético que afectó su infraestructura informática, según fuentes abiertas. Como medida de seguridad, se restringió temporalmente el acceso a sus sistemas para mitigar riesgos. Este incidente provocó la interrupción de operaciones clave, incluyendo el registro de información contable y pagos a proveedores y empleados. El Sistema de Contabilidad Integrada (SICOIN) permaneció inoperativo por más de 40 horas.

2. **Incremento de ciberataques a empresas – 2023**

   En 2023, se reportó que aproximadamente el 40% de los ciberataques en Guatemala estuvieron dirigidos a empresas, según medios de comunicación. Estos ataques afectaron la facturación, el pago de impuestos y procesos en aduanas, evidenciando la creciente amenaza que representan los delitos cibernéticos para el sector privado.

3. **Ataque al Ministerio de Educación (MINEDUC) – Agosto 2024**

   El 30 de agosto de 2024, el MINEDUC informó sobre un ataque cibernético a sus sistemas informáticos, según medios de comunicación. La cartera educativa procedió con la protección de datos y la ejecución de programas, además de presentar la denuncia correspondiente ante las autoridades competentes.

4. **Infiltración al Ministerio de Relaciones Exteriores (MINEX) – Septiembre 2022 a Febrero 2025**

   Según medios de comunicación nacionales e internacionales, una revisión conjunta entre el Gobierno de Guatemala y el Comando Sur de los Estados Unidos de América, identificó que grupos de espionaje cibernético con sede en la República Popular de China infiltraron los sistemas informáticos del MINEX, desde septiembre de 2022 hasta febrero de 2025. Estos hackers accedieron a datos oficiales, aunque no se ha divulgado el alcance exacto de la información comprometida.

   El Presidente Bernardo Arévalo, destacó la detección de estas amenazas durante un ejercicio cibernético conjunto con Estados Unidos y Taiwán, subrayando la necesidad de fortalecer la ciberseguridad nacional.

El contexto anterior, evidencia que las organizaciones deben fortalecer sus capacidades, especialmente, las acciones preventivas y reactivas. Así como, la coordinación a nivel político, estratégico, operativo y tecnológico, con el fin de gestionar el desarrollo de políticos y estrategias de ciberseguridad.

Las instituciones del sector público, en su mayoría, cuentan con sistemas gubernamentales desactualizados, con bajo o nulo control en materia de ciberseguridad, ya que el país carece de

una institucionalidad que permita la definición e identificación de su infraestructura critica fisica y digital. Por otro lado, el sector privado, ha avanzado en el desarrollo de sus capacidades, especialmente, el sector financiero, el cual ha sido el más vulnerable ante los incidentes cibernéticos. No obstante, es necesario crear los mecanismos legales, operativos y tecnológicos para una atención integral a la problemática.

II. CONTENIDO DE LA INICIATIVA DE LEY

La estructura de este cuerpo normativo y el proceso de formulación de la iniciativa de ley refiere lo siguiente:

Que el ordenamiento jurídico guatemalteco debe responder a los avances de las tecnologías de la información y las comunicaciones, correspondiendo al Estado crear la legislación especial al ámbito de actuación, que defina las conductas delictivas, aplicando su poder coercitivo, con lo cual se pueda garantizar, prevenir, la violación y vulneración de derechos y bienes jurídicos.

Crear un cuerpo normativo complementario que proteja y resguarde los datos personales, la intimidad informática, los datos comerciales, bancarios y financieros, la confidencialidad, la integridad y disponibilidad de la información. Así como, los datos contenidos en sistemas informáticos o sistemas que empleen tecnologías de la información y las comunicaciones. También, el resguardo y la integración de los procedimientos que garanticen el Estado de Derecho y debido proceso, estableciendo las funciones y competencias necesarias de las entidades del sector justicia y administrativas, contemplando, normas que favorecen la cooperación internacional en materia de ciberseguridad.

Siendo el objeto de esta la tipificación de conductas delictivas, para prevenir, erradicar y sancionar los ciberdelitos; velar por el desarrollo de las capacidades de ciberseguridad y ciberdefensa. Así como, se estipulan reglas procesales necesarias para incorporar los medios de prueba digitales que permitan la obtención de evidencias y pruebas electrónicas en el proceso penal, para una investigación eficaz y la cooperación interinstitucional e internacional en la materia.

III. CONSIDERACIONES DE ORDEN CONSTITUCIONAL Y LEGAL:

CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE GUATEMALA

Artículo 1. Protección a la Persona. El Estado de Guatemala se organiza para proteger a la persona y a la familia; su fin supremo es la realización del bien común.

Artículo 2. Deberes del Estado. Es deber del Estado garantizarles a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona.

Artículo 24. Inviolabilidad de correspondencia, documentos y libros. (...) Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna...

Artículo 46. Preeminencia del Derecho Internacional. Se establece el principio general de que en materia de derechos humanos, los tratados y convenciones aceptados y ratificados por Guatemala, tienen preeminencia sobre el derecho interno.

Artículo 244. Integración, organización y fines del Ejército. El Ejército de Guatemala, es una institución destinada a mantener la independencia, la soberanía y el honor de Guatemala, la integridad del territorio, la paz y la seguridad interior y exterior.

CÓDIGO PENAL

Artículo 173 Bis. Quién con violencia física o sicológica, realice actos con fines sexuales o eróticos a otra persona, al agresor o a sí misma, siempre que no constituya delito de violación (...) Siempre se comete este delito cuando la víctima sea una persona menor de catorce años de edad o cuando sea una persona con incapacidad volitiva o cognitiva aun cuando no medie violencia física o psicológica...

Artículo 188 Quien ejecute, o hiciere ejecutar a otra persona, actos sexuales frente a personas menores de edad o persona con incapacidad volitiva o cognitiva,...

Artículo 189 (...) quien: a. Permita presenciar espectáculos de naturaleza sexual reservados para adultos, a personas menores de edad o con incapacidad volitiva o cognitiva. b. Permita a menores de edad el ingreso a espectáculos públicos de naturaleza sexual, reservados para adultos. c. De cualquier forma distribuya a personas meno res de edad material pornográfico. d. De cualquier forma permita adquirir material pornográfico a personas menores de edad.

Artículo 190. Delito de violación a la intimidad sexual. Segundo párrafo: (...) se apodere, acceda, utilice o modifique, en perjuicio de tercero, comunicaciones efectuadas por cualquier medio físico o electrónico o datos reservados con contenido sexual de carácter personal, familiar o de otro, que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos...

Artículo 193 Ter. Quien de cualquier forma y a través de cualquier medio produzca, fabrique o elabore material pornográfico que contenga imagen o voz real o simulada de una o varias personas menores de edad o con incapacidad volitiva o cognitiva, en acciones pornográficas o eróticas, será sancionado con...

Artículo 195 Bis. Quien publique, reproduzca, importe, exporte, distribuya, transporte, exhiba, elabore propaganda, difunda o comercie de cualquier forma y través de cualquier medio, material pornográfico de personas menores de edad o con incapacidad volitiva o cognitiva en donde se utilice su imagen o voz real o simulada, será sancionado con...

Artículo 195 Ter. Quien a sabiendas posea y adquiera material pornográfico, de una o varias personas menores de edad o con incapacidad volitiva o cognitiva, en acciones pornográficas o eróticas, será sancionado con...

Artículo 196. Comete el delito de publicaciones y espectáculos obscenos quien contra la moral por la razón de exponerlos a la vista de menores de edad y del público, publicare y difundiere por cualquier medio, fabricare, reprodujere o vendiere: libros, escritos, imágenes, gráficos u otros objeto pornográficos y obscenos...

Artículo 274. Salvo los casos contemplados expresamente en leyes o tratados sobre la materia de los que la República de Guatemala sea parte (...) quien realice cualquiera de los actos siguientes: (...) h) La fijación, reproducción o retransmisión de una difusión transmitida por satélite, radio, hilo, cable, fibra óptica o cualquier otro medio sin la autorización del titular del derecho; i) La comunicación al público de una difusión o transmisión en un sitio al que el público pueda tener acceso pagando una cuota de admisión, o con el fin de consumir o adquirir productos o ser vicios, sin la autorización del titular del derecho correspondiente; (...) k) Manufacture, ensamble, modifique, importe, exporte, venda, arrende o de cualquier forma distribuya un dispositivo o sistema tangible o intangible, sabiendo o teniendo razón para saber que el dispositivo o sistema sirve o asiste principalmente para decodificar una señal de satélite codificada, que tenga un programa sin la autorización del distribuidor legal de dicha señal, o la recepción y distribución intencionada de una señal que lleva un programa que se originó como señal satelital codificada, sabiendo que fue decodificada, sin la autorización del distribuidor legal de la señal...

Artículo 274 "A". (...) quien destruya, borre o de cualquier modo inutilice, altere o dañe registros informáticos.

Artículo 274 "B". (...) al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras.

Artículo 274 "C". (...) al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

Artículo 274 "D". (...) al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Artículo 274 "E". (...) al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.

ARTÍCULO 274 "F". (...) al que, sin autorización, utilice u obtenga para sí o para otro, datos contenidos en registros informáticos, bancos de datos o archivos electrónicos.

Artículo 274 "G". (...) al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

Artículo 274 "H". Quien mediante cualquier mecanismo altere el número proveniente de un operador extranjero de telefonía utilizado exclusivamente para tráfico internacional, o altere el número de identificación del usuario que origine una llamada de telefonía...

Artículo 275 Bis. Toda persona individual o jurídica que comercialice los terminales móviles que hayan sido reportados como robados o hurtados y que aparezcan en la BDTR (lista negra) establecida por cada operador, así como toda persona que reprograme o en cualquier forma modifique, altere o reproduzca en dichos terminales móviles, el Número Serial Electrónico (ESN) del equipo terminal móvil, el Número de Identidad de Equipo Móvil Internacional (IMEI), para el Sistema Global para Comunicaciones Móviles (GSM), o cualquier otra característica de identificación propia de los terminales móviles, o reprograme, altere o reproduzca en forma fraudulenta cualquier Módulo de Identidad del Suscriptor (SIM) para el Sistema Global para Comunicaciones Móviles (GSM), será responsable del delito de alteración fraudulenta...

Artículo 303 Quáter. (...) Quien almacene, distribuya, importe, exporte, comercialice, transporte, venda, dispense o ponga a disposición del público por cualquier medio, incluyendo los electrónicos o informáticos, medicamentos, productos farmacéuticos, dispositivos médicos o material médico quirúrgico que han sido producidos, manufacturados, fabricados, empacados, envueltos, acondicionados y/o etiquetados en forma fraudulenta...

CÓDIGO PROCESAL PENAL

Artículo 198. Entrega de cosas y secuestro. Las cosas y documentos relacionados con el delito o que pudieran ser de importancia para la investigación y los sujetos a comiso serán depositados y conservados del mejor modo posible. Quien los tuviera en su poder estará obligado a presentarlos y entregarlos a la autoridad requirente. Si no son entregados voluntariamente, se dispondrá su secuestro.

Así también:

LEY DE PROPIEDAD INDUSTRIAL

LEY DE DERECHOS DE AUTOR Y DERECHOS CONEXOS

LEY MARCO DEL SISTEMA NACIONAL DE SEGURIDAD, DECRETO 18-2008 DEL CONGRESO DE LA REPÚBLICA.

IV. NORMAS INTERNACIONALES:

ISO 27035 de aplicación en cualquier ámbito a la hora de llevar a cabo la gestión de incidentes de seguridad:

- Detección y gestión de los eventos de seguridad que se produzcan determinando si corresponden o no a un incidente;

- Respuesta a los incidentes de forma proporcional, ágil y adecuada de manera que se minimice el impacto asociado a los incidentes acontecidos; y,
- Extracción de lecciones aprendidas a partir de los incidentes gestionados de forma que se mejore el estado global de la seguridad corporativa incluyendo la optimización de los procedimientos de gestión de incidentes.

NIST acrónimo del Instituto Nacional de Estándares y Tecnología en inglés *National Institute of Standards and Technology*, organismo dependiente del Departamento de Comercio de Estados Unidos:

- Identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica;
- Proporcionar un enfoque prioritario, flexible, repetible, basado en el rendimiento y rentabilidad;
- Ayudar a identificar, evaluar y gestionar el riesgo cibernético;
- Incluir orientación para medir el desempeño de la implementación del marco de ciberseguridad; y,
- Identificar áreas de mejora que deben abordarse a través de la colaboración futura con sectores particulares y organizaciones que desarrollan estándares. (García M. M., 2022).

V. ANÁLISIS DE LA COMISIÓN

La ciberseguridad reviste una importancia estratégica al comprender la aplicación coordinada de técnicas, herramientas y políticas orientadas a proteger las infraestructuras físicas y digitales, frente a posibles ataques, accesos no autorizados o amenazas que puedan comprometer su integridad, disponibilidad o confidencialidad. En ese sentido, la protección de los sistemas informáticos y tecnologías de la información y comunicación, son esenciales para el ejercicio de derechos fundamentales, el funcionamiento institucional y la preservación del patrimonio digital.

La tipificación actual de los delitos informáticos contenidos en el Código Penal, Ley de Propiedad Industrial y Ley de Derechos de Autor y Derechos Conexos, no responden a las modalidades de los ilícitos que se cometen a través de redes, sistemas informáticos y tecnologías de la información y comunicación. En la actualidad, la legislación internacional, contempla delitos como: el acceso ilícito, la interceptación ilícita, el abuso de dispositivos, entre otros. La ausencia de una legislación específica que tipifique los ciberdelitos se convierte en un incentivo a los ciberdelincuentes, los cuales utilizan vacíos legales para actuar con impunidad.

Para garantizar el Estado de Derecho, Guatemala, debe establecer los tipos penales, las penas y el debido proceso en materia de ciberdelitos, para garantizar a los ciudadanos el cumplimiento de los preceptos constitucionales y aquellos principios como el de celeridad, oralidad, inmediación, publicidad, contradictorio y debido proceso, que se derivan de la Constitución Política de la República de Guatemala.

En virtud de esa obligatoriedad constitucional se deben establecer previamente los tipos penales, las penas y una debida persecución de estos, con la finalidad de establecer el bien común, desde

una percepción de justicia y de integridad de los principios y los derechos humanos. Así como, el fortalecimiento de las capacidades para el sector justicia para la prevención, persecución y sanción en materia de ciberseguridad. Una legislación que aborde la materia de ciberseguridad, especialmente la tipificación de ciberdelitos incrementa la capacidad para actuar y colaborar con otros países en la persecución de estos.

La presente iniciativa de Ley de Ciberseguridad tiene el potencial de prevenir diversos delitos en el entorno digital, como: el acceso no autorizado a sistemas informáticos, el robo de datos personales, el fraude financiero y otros actos ilícitos tipificados en esta normativa.

Este marco legal, establece sanciones claras para los responsables, contemplando el incremento de las penas en función de los agravantes presentes en cada caso y perfil de las personas involucradas en la comisión de estos actos. Por ejemplo, cuando sea cometido por una persona que preste o haya prestado sus servicios, directa o indirectamente, a la persona individual o jurídica afectada, o sea cometido por empleado o funcionario público.

Asimismo, si la acción se realiza en contra de las instituciones del Sistema Nacional de Seguridad u otras instituciones del Estado, o que ponga en peligro y afecte la funcionalidad de las infraestructuras críticas físicas o digitales, sin perjuicio de las sanciones que establezca la legislación en materia de responsabilidades administrativa.

El catálogo de delitos cibernéticos que contempla esta iniciativa contribuye, tanto a su prevención específica como general. Respalda la investigación y persecución de dichos delitos mediante el trabajo de instituciones especializadas, conforme a lo dispuesto en esta legislación y en el ordenamiento jurídico vigente, e incrementa en una cuarta parte las penas aplicables a los responsables de los delitos tipificados en el Decreto Número 57-2000, Ley de Propiedad Industrial; el Decreto Número 33-98, Ley de Derechos de Autor y Derechos Conexos; y, en los delitos contemplados en el Título VI, Capítulo VII del Decreto Número 17-73, Código Penal. Este aumento se aplica cuando dichos delitos son perpetrados a escala comercial utilizando sistemas informáticos o tecnologías de la información y comunicaciones.

Es importante destacar que la iniciativa de Ley de Ciberseguridad dispone que los delitos establecidos en los artículos 173 bis, 188, 189, 190, 192, 195 Bis, 195 Ter y 196 del Decreto Número 17-73 del Congreso de la República, Código Penal, sean cometidos utilizando sistemas informáticos o tecnologías de la información y comunicación, las penas correspondientes se incrementarán conforme a lo establecido en el artículo 195 Quinquies del citado cuerpo legal.

El Centro de Respuesta a Incidentes de Seguridad Informática de Guatemala -CSIRT-GT-, es la institucionalidad más relevante de la presente iniciativa, cuyo acrónimo proviene del término inglés *Computer Security Incident Response Team*, seguido del identificador nacional *GT*, en concordancia con los estándares internacionales en materia de ciberseguridad. Este Centro se constituirá como el órgano técnico responsable de la detección, análisis, gestión, coordinación y respuesta ante incidentes de ciberseguridad en el territorio nacional. Cumpliendo con las siguientes funciones:

a) Monitoreo permanente para la atención de incidentes cibernéticos y ciberataques;
b) Asegurar la continuidad operativa y rendimiento de la red y sistemas de las infraestructuras críticas a nivel nacional;
c) Prestar servicios proactivos de ciberseguridad;
d) Prestar servicios reactivos de ciberseguridad;
e) Prestar servicios post incidentes cibernéticos y ciberataques;
f) Detectar, investigar y mitigar incidentes cibernéticos y ciberataques;
g) Coordinar con los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT´s) internacionales, sectoriales e institucionales;
h) Dar respuesta a incidentes cibernéticos y ciberataques que atenten contra la integridad, confidencialidad y disponibilidad de los sistemas que hagan uso de tecnologías de la información y comunicación a nivel nacional;
i) Rendir informes periódicos y específicos al Consejo Nacional de Seguridad, sobre la atención, seguimiento y resolución de ciberataques e incidentes cibernéticos gestionados;
j) Establecer y actualizar los procedimientos para la prevención, detección, análisis, contención, mitigación y recuperación de ciberataques e incidentes cibernéticos;
k) Identificar, clasificar, analizar y evaluar la gravedad de ciberataques e incidentes cibernéticos a nivel nacional;
l) Emitir alertas e informar oportunamente a los potenciales afectados de ciberataques e incidentes cibernéticos;
m) Colaborar con los procesos continuos de auditoría de ciberseguridad en las instituciones del Estado, garantizando la identificación, prevención, protección, detección, preparación, recuperación y respuesta de vulnerabilidades;
n) Elaborar informes, coordinar y dar seguimiento en los casos atendidos; brindando asistencia técnica, según corresponda;
o) Realizar ejercicios y simulacros para la atención de ciberataques e incidentes cibernéticos;
p) Elaborar el Código de Ética para los actores involucrados en la ciberseguridad; y,
q) Otras que de acuerdo con la evolución de la ciberseguridad y el reglamento correspondientes sean necesarias.

Desde una perspectiva sistemática, el diseño e implementación de la Ley de Ciberseguridad, requiere un marco normativo y sustantivo, para el fortalecimiento institucional de los órganos responsables de su aplicación. El presente análisis identifica las siguientes propuestas como fundamentales para su operatividad efectiva:

- **Ministerio Público**: se establece la creación de una *Fiscalía Especializada en Ciberdelincuencia*, con competencia funcional para la investigación penal, la formulación de requerimientos y el litigio estratégico de los delitos contemplados en el ámbito digital.
- **Instituto Nacional de Ciencias Forenses (INACIF)**: se propone la conformación de una *unidad especializada para la investigación científica forense*, encargada de la obtención,

análisis y validación de pruebas científicas en procesos de investigación forense vinculados con delitos informáticos.

- **Organismo Judicial**: se impulsa la instalación y operación de *Órganos Jurisdiccionales Especializados en Ciberseguridad*, con dotación adecuada de infraestructura tecnológica, soporte logístico y personal capacitado, garantizando la tutela judicial efectiva y especializada.
- **Instituto de la Defensa Pública Penal**: se dispone la incorporación de profesionales del derecho con formación especializada en ciberdelitos, asegurando una defensa técnica idónea conforme a los principios del debido proceso y acceso a la justicia.
- **Policía Nacional Civil**: se instruye la creación de la *Dirección de Ciberseguridad y Ciberdelincuencia*, como dependencia especializada responsable de la prevención, detección, investigación y respuesta ante conductas delictivas digitales, conforme a estándares técnicos y principios de legalidad.

Los delitos informáticos, transcienden fronteras, lo que plantea un desafío a la soberanía jurídica y a los modelos tradicionales de justicia penal. En este contexto, la Ley de Ciberseguridad incorpora mecanismos de cooperación internacional, como instrumentos sustantivos, necesarios para garantizar la aplicación efectiva del orden jurídico nacional en entornos digitales transfronterizos.

Desde una perspectiva normativa, se establece la regulación de procedimientos vinculados a la extradición activa y pasiva, conforme al marco legal interno y a los tratados internacionales en materia penal de los que Guatemala es parte; disposición que resulta esencial para la articulación de la jurisdicción penal, en casos donde los perpetradores se encuentren fuera del territorio nacional, pero sus acciones tengan efectos jurídicos locales.

Además, se prevé una arquitectura de asistencia judicial internacional que abarca:

a) La solicitud de aseguramiento y conservación de datos digitales que puedan constituir medios probatorios;
b) La presentación, acceso controlado y confiscación de datos, conforme a requerimientos específicos emitidos por autoridades extranjeras y avalados por tratados vigentes;
c) El acceso libre a información de fuentes abiertas, siempre que dicho acceso se realice bajo los principios de legalidad, proporcionalidad y respeto a la autodeterminación informativa; y,
d) El intercambio de datos sobre tráfico e interceptación de comunicaciones, bajo protocolos que aseguren la trazabilidad, la confidencialidad y el respeto a los derechos fundamentales.

Este régimen jurídico internacional se fundamenta en el principio de *cooperación activa*, y su eficacia depende de la armonización entre el *derecho interno guatemalteco* y los *instrumentos multilaterales*, firmados y ratificados por el Estado de Guatemala. Por lo tanto, consolida el compromiso del Estado, con la protección global de los derechos digitales y la construcción de entornos seguros en el ciberespacio.

Desde una perspectiva institucional, este enfoque demanda capacidades técnicas, normativas y diplomáticas que habiliten a las entidades competentes para atender solicitudes internacionales

de manera ágil y conforme a estándares internacionales, garantizando con ello la efectividad del sistema de justicia frente a delitos digitales.

Con base en lo dispuesto por el artículo 244 de la Constitución Política de la República de Guatemala, que establece al Ejército como la institución encargada de mantener la independencia, la soberanía, el honor nacional, la integridad territorial; así como la paz y la seguridad tanto interior como exterior. Corresponde al Ministerio de la Defensa Nacional, implementar de forma permanente las acciones para la ciberdefensa, asegurando la resiliencia de los sistemas digitales y la soberanía nacional en el ámbito del ciberespacio.

Dentro de ese orden de ideas, esta iniciativa de ley también contempla lo relativo a la ciberdefensa, con las siguientes funciones:

a) Dar protección preventiva y activa de redes militares y sistemas informáticos y tecnologías de la información y la comunicación que integren las infraestructuras críticas que atenten contra la Defensa Nacional;
b) Desarrollar acciones defensivas y ofensivas para la protección de las infraestructuras críticas que atenten contra la Defensa Nacional, conforme lo determine el Consejo Nacional de Seguridad, presidido por el Presidente de la República;
c) Planificar, identificar, recolectar, procesar, analizar, producir, distribuir y difundir información de manera oportuna para la ciberdefensa, estableciendo los protocolos necesarios;
d) Dar apoyo a las operaciones militares de tierra, aire y mar;
e) Mantener comunicación y coordinación permanente con el CSIRT-GT;
f) Coordinar con los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT´s) internacionales, sectoriales e institucionales, públicos y privados, en aquellos casos que se afecte las infraestructuras críticas, conforme lo determine el Presidente de la República en Consejo Nacional de Seguridad;
g) Dar apoyo al CSIRT-GT en aquellos casos en que sus capacidades técnicas u operativas sean sobrepasadas, conforme lo determine el Consejo Nacional de Seguridad, presidido por el Presidente de la República;
h) Ser el punto de contacto a nivel internacional en materia de ciberdefensa, para brindar seguimiento, apoyo y recomendaciones, cuando le sea requerido;
i) Crear los marcos normativos y la doctrina para la ciberdefensa;
j) Establecer y actualizar, los protocolos y estándares, para la prevención, detección, contención, protección, recuperación de los sistemas y respuesta del Ministerio de la Defensa Nacional;
k) Diseñar y realizar programas de formación continua, entrenamiento especializado, simulacros técnicos y ejercicios conjuntos en materia de ciberdefensa, a nivel nacional e internacional;
l) Rendir informes al Consejo Nacional de Seguridad, mensualmente o cuando sean necesarios, sobre la atención, seguimiento y resolución de los incidentes gestionados para la ciberdefensa; y,
m) Asesorar técnicamente en el diseño de políticas, estrategias, programas y acciones en materia de ciberdefensa.

CONGRESO DE LA REPÚBLICA

COMISIÓN DE ASUNTOS DE SEGURIDAD NACIONAL

En el marco de la Ley de Ciberseguridad, contenida en la iniciativa 6347, se propone la derogación de los artículos 274 "A", 274 "B", 274 "C", 274 "E", 274 "F" y 274 "G" del Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, debido a su obsolescencia normativa. Los artículos en mención fueron concebidos en un entorno tecnológico limitado, sin considerar las dinámicas actuales del ciberespacio, sus definiciones y sanciones no reflejan la complejidad de los delitos informáticos contemporáneos, ni las nuevas formas de evidencia digital. En contraste, la iniciativa 6347 establece un marco jurídico integral y actualizado que tipifica conductas como el acceso ilícito, la interceptación de datos, la manipulación de sistemas informáticos, el fraude digital, entre otros, conforme a estándares internacionales. La coexistencia de ambas regulaciones generaria confusión jurídica, al crear un régimen normativo paralelo con definiciones técnicas y penas divergentes para conductas similares.

En coherencia con el fortalecimiento del marco legal en materia de seguridad nacional, la presente iniciativa de ley adiciona la literal i) al artículo 2 del Decreto Número 21-2006 del Congreso de la República, Ley Contra la Delincuencia Organizada. La nueva disposición quedará redactada de la siguiente forma:

"i) *De los contenidos en la Ley de Ciberseguridad: acceso ilícito; intercepción ilícita; ataque a la integridad de los datos informáticos; ataque a la integridad del sistema informático; falsificación informática; apropiación de identidad ajena; fraude informático; y, abuso de dispositivos; así como otros delitos tipificados en la Ley de Ciberseguridad y en demás cuerpos normativos relacionados con la materia.*"

En lo relativo al presupuesto, las instituciones del Estado mencionadas en esta ley deberán incluir cada año, en su planificación presupuestaria, los recursos necesarios para cumplir con las funciones que esta norma les asigna y en caso de no contar con la asignación suficiente, deberán realizar los ajustes necesarios dentro de su propio presupuesto, con el fin de asegurar la disponibilidad de fondos para ejecutar adecuadamente las actividades establecidas en esta ley, conforme a la normativa vigente en materia presupuestaria.

Además, queda expresamente establecido que las adquisiciones de bienes, equipos, sistemas o tecnologías destinadas a la Ciberseguridad y Ciberdefensa deberán realizarse bajo reserva, en virtud de su carácter estratégico y por estar vinculadas a la seguridad nacional. Dichas compras estarán sujetas a los regímenes especiales de contratación establecidos en la legislación aplicable, garantizando la confidencialidad, protección de la información y el interés superior del Estado.

Se considera que establecer un marco legal sólido, fortalece la cooperación interinstitucional e internacional, permitiendo la persecución eficaz de los delitos de ciberseguridad. La implementación de un Centro de Respuesta a Incidentes de Seguridad Informática de Guatemala -CSIRT-GT-, proporcionará un punto de contacto centralizado, facilitando la resolución de incidentes de seguridad en cualquier institución, agilizando la respuesta a nivel nacional e internacional.

Asimismo, deberá elaborarse el Reglamento de la Ley de Ciberseguridad, el cual establecerá, entre otros aspectos, las competencias específicas de las instituciones creadas, los mecanismos de coordinación interinstitucional, así como, los criterios técnicos para la implementación de medidas de ciberseguridad. Dicho cuerpo normativo también regulará aspectos complementarios necesarios para la operatividad de la ley, incluyendo los estándares técnicos aplicables, los mecanismos de supervisión y control, los procedimientos sancionatorios, y demás disposiciones que resulten esenciales para garantizar su adecuada ejecución. La elaboración de este reglamento corresponderá a la autoridad competente, conforme al procedimiento legal establecido.

Resulta oportuno informar al Honorable Pleno que este proyecto de ley ha sido objeto de un amplio proceso de discusión y análisis con diversas instituciones públicas y privadas, así como con expertos en la materia; proceso en el que participaron:

Ministerio Público

1. Secretaría de Política Criminal;
2. Fiscales de Narcoactividad;
3. Fiscales de Crimen Organizado;
4. Fiscales de Delitos Económicos;
5. Fiscales de Lavado de Dinero;
6. Fiscales de Delitos Transnacionales;

Dirección General de la Policía Nacional Civil

7. Departamento de Investigación de Ciberdelitos;
8. Subdirección General de Tecnologías de la Información y Comunicación;

Comité Nacional de Seguridad Cibernética -CONCIBER-

9. Ministerio de Gobernación -IV Viceministerio-;
10. Ministerio de Relaciones Exteriores;
11. Ministerio de la Defensa Nacional;
12. Secretaría de Inteligencia Estratégica del Estado;
13. Secretaría Técnica del Consejo Nacional de Seguridad;
14. Comisión Presidencial de Gobierno Abierto y Electrónico;
15. Superintendencia de Bancos;
16. Superintendencia de Telecomunicaciones;

Ministerio de la Defensa Nacional

17. Dirección General de Política de Defensa;
18. Brigada de Comunicaciones e Informática del Ejército de Guatemala;

Otros:

19. Jueces de Mayor Riesgo;
20. Instituto Nacional de Ciencias Forenses (INACIF);
21. Banco de Guatemala (BANGUAT);
22. Asociación Bancaria de Guatemala (ABG);
23. Comunidad Bancaria de Ciberseguridad (BANCERT);
24. Observatorio Tecnológico de Guatemala, que incluye 300 participantes de gobierno, academia, sociedad civil, empresas nacionales e internacionales que reúnen alrededor de 1,700 participantes;
25. Foro Parlamentario de Transformación Digital del Congreso de la República de Guatemala;
26. Asociación Guatemalteca de Exportadores (AGEXPORT);
27. Profesionales del Derecho;
28. Tanques de Pensamiento Nacionales;
29. Centro de Estudios de Defensa Hemisférica William J. Perrry -Departamento de Estado de Estados Unidos-;
30. Embajada de Estados Unidos de América;
31. Equipo de Ciberseguridad de la Embajada de Estados Unidos de América;
32. Embajada de Taiwán;
33. Unión Europea; y,
34. Expertos en Ciberseguridad de Guatemala, Estados Unidos y Chile.

La promulgación de la Ley de Ciberseguridad es imprescindible, su propósito será regular la integración, organización y funcionamiento de una entidad encargada de las actividades de ciberseguridad a nivel nacional, guiada por principios rectores, estableciendo las bases para la coordinación y colaboración entre las instituciones del Estado. Promoverá el uso seguro y responsable de las redes, sistemas de información y comunicaciones, fortaleciendo las capacidades de prevención, detección y respuesta ante ciberataques, mediante la adopción de medidas específicas para consolidar un ciberespacio seguro.

VI. DICTAMEN

Luego de la discusión, estudio y análisis del contenido de la Iniciativa de Ley número 6347, que tiene como objetivo establecer un marco jurídico para regular los ciberdelitos, el tratamiento de pruebas digitales y la respuesta ante incidentes cibernéticos, con base en los artículos 39, 40 y 41 de la Ley Orgánica del Organismo Legislativo, fundamento legal y consideraciones vertidas anteriormente, la Comisión de Asuntos de Seguridad Nacional del Congreso de la República, emite su **DICTAMEN FAVORABLE CON MODIFICACIONES** a la **iniciativa que dispone aprobar Ley de Ciberseguridad**; el cual, se somete a consideración del Honorable Pleno del Congreso de la República de Guatemala para lo que en ley corresponde.

Guatemala, 26 de agosto de 2025.

CONGRESO DE LA REPÚBLICA

COMISIÓN DE ASUNTOS DE SEGURIDAD NACIONAL

Jorge Mario Villagrán Álvarez
Presidente

Rodrigo Antonio Pellecer Rodríguez
Vicepresidente

Luis Javier López Bolaños
Secretario

Mirna Victoria Godoy Palala
Integrante

Voto Razonado a favor

Darwin Alberto Lucas Paz
Integrante

Víctor Alfredo Valenzuela Argueta
Integrante

León Felipe Barrera Villanueva
Integrante

Nery Abilio Ramos y Ramos
Integrante

Allan Estuardo Rodríguez Reyes
Integrante

Felipe Alejos Lorenzana
Integrante

José Pablo Mendoza Franco
Integrante

Adim Maldonado Molina
Integrante

CONGRESO DE LA REPÚBLICA

DECRETO NÚMERO ___-2025

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO

Que es deber constitucional del Estado garantizar a los habitantes de la República, la libertad, la justicia, la seguridad y el desarrollo integral de las personas. Asimismo, se organiza para la protección de las personas y sus bienes, lo cual en la era digital incluye la protección en el ciberespacio;

CONSIDERANDO

Que Guatemala ha experimentado un crecimiento exponencial en el uso de tecnologías de la información y comunicación, así como en la digitalización de servicios públicos y privados, lo que genera nuevos riesgos, amenazas y vulnerabilidades que requieren un marco normativo especializado;

CONSIDERANDO

Que la investigación y persecución de delitos informáticos requiere de marcos normativos actualizados, capacidades técnicas especializadas y mecanismos de cooperación nacional e internacional que permitan una respuesta multidominio ante estos riesgos y amenazas.

CONSIDERANDO

Que es imprescindible establecer mecanismos de intercambio de información sobre riesgos y amenazas cibernéticas entre entidades públicas y privadas, respetando la confidencialidad y protección de datos sensibles, para fortalecer la capacidad de respuesta integral;

POR TANTO:

En ejercicio de las atribuciones que le confiere el artículo 171 literal a) de la Constitución Política de la República de Guatemala,

DECRETA:

"LEY DE CIBERSEGURIDAD"

TÍTULO I

DISPOSICIONES GENERALES Y ELEMENTOS CONCEPTUALES

CAPÍTULO I

OBJETO Y ÁMBITOS DE APLICACIÓN

Artículo 1. Objeto de la ley. La presente ley tiene por objeto, crear y desarrollar las capacidades e institucionalidad para el abordaje de la ciberseguridad; tipificación de conductas delictivas para prevenir, sancionar y erradicar los ciberdelitos; establecer reglas procesales para obtener e incorporar evidencia y prueba al proceso penal; así como, establecer la cooperación interinstitucional e internacional en la materia.

Artículo 2. Bienes jurídicos tutelados. Son bienes jurídicos tutelados en la presente ley los siguientes:

a) El patrimonio, la privacidad de las personas y la protección de niñas, niños y adolescentes;
b) Confidencialidad, integridad y disponibilidad de los datos, comunicaciones, dispositivos electrónicos y sistemas informáticos; y,
c) El Estado y sus instituciones.

Artículo 3. Ámbito de aplicación. El ámbito de aplicación de la presente ley, lo constituye todo el territorio de la República de Guatemala, siendo su aplicación extensiva a toda persona individual y jurídica, nacional o extranjera, que cometa un hecho tipificado como delito en el ciberespacio, en cualquiera de las condiciones o circunstancias siguientes:

a) Cuando el sujeto activo origina, ordena o ejecuta la acción delictiva dentro del territorio nacional;
b) Cuando el sujeto activo origina, ordena o ejecuta la acción delictiva desde el extranjero, produciendo su consumación o sus efectos dentro del territorio nacional;
c) Cuando el origen o los efectos de la acción se produzca en el extranjero, utilizando medios que se encuentran en el territorio nacional;
d) Cuando se materialice o evidencie cualquier tipo de participación desde el territorio guatemalteco, con un acto, sin el cual no se hubiere podido cometer la acción delictiva.

Artículo 4. Definiciones. Además de las definiciones contenidas en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008 del Congreso de la República de Guatemala, y para los efectos de la presente ley, se entenderá por:

a) **Ciberamenaza:** fuente potencial de perjuicio, externa o interna, al Estado, que se materializa a través del ciberespacio.
b) **Ciberarma:** herramienta digital o software diseñado específicamente para realizar ciberataques, comprometiendo la seguridad de sistemas de información.
c) **Ciberataque:** uso deliberado de una ciberarma, por una persona o de manera automática, para causar un daño o efecto perjudicial a un elemento del ciberespacio de un adversario, pudiendo tener efectos indirectos en el funcionamiento de los sistemas de información afectados.

d) **Ciberdefensa:** el empleo de las capacidades militares ante las amenazas o actos hostiles de naturaleza cibernética, los cuales afectan las infraestructuras críticas, a la sociedad, la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales.
e) **Ciberdelincuencia**: conjunto de acciones ilícitas realizadas a través del ciberespacio que vulneran la confidencialidad, integridad o disponibilidad de los sistemas de información, redes y medios de comunicación. Estas conductas tienen como finalidad la apropiación, destrucción, alteración o uso no autorizado de bienes, datos o derechos de las personas o entidades afectadas.
f) **Ciberdelitos:** conductas típicas, antijuridicas, culpables y punibles que utilizan los sistemas informáticos o tecnologías de la información y la comunicación con el objeto de lesionar bienes o derechos de la víctima.
g) **Ciberespacio:** dominio global del entorno de la información, conformado por una red interconectada e interdependiente de infraestructuras tecnológicas. Incluye internet, redes de telecomunicaciones, sistemas informáticos, así como dispositivos, procesadores y controladores integrados que permiten el almacenamiento, procesamiento y transmisión de datos digitales.
h) **Ciberseguridad:** conjunto de políticas, estrategias, procedimientos, medidas técnicas y capacidades institucionales orientadas a proteger, defender y garantizar la resiliencia del ciberespacio. Comprende la prevención, detección, respuesta y recuperación frente a riesgos, amenazas, vulnerabilidades o actividades maliciosas que afecten sistemas informáticos o cualquier infraestructura que utilice tecnologías de la información y la comunicación. Su finalidad es preservar la confidencialidad, integridad y disponibilidad de la información, así como, salvaguardar la seguridad nacional, la estabilidad económica y el orden público.
i) **Confidencialidad:** atributo de la información que busca prevenir su acceso, uso o divulgación por parte de personas no autorizadas, garantizando que únicamente quienes cuenten con la debida autorización puedan acceder a ella.
j) **Datos de tráfico:** cualquier forma de información digital que se esté transmitiendo, a través de redes o canales de comunicación. Estos datos pueden circular dentro o fuera del perímetro de una organización e incluyen las comunicaciones entre computadoras, servidores u otros dispositivos en el ciberespacio.
k) **Datos informáticos:** toda representación de hechos, instrucciones, caracteres, o conceptos expresados de cualquier forma que se preste a tratamiento informático. Incluye tanto los datos como los programas diseñados para que un sistema informático ejecute una función.
l) **Disponibilidad:** atributo de la información que garantiza que los sistemas, servicios y datos estén accesibles y operativos cuando se necesiten, por personas o entidades autorizadas, sin interrupciones indebidas.
m) **Dispositivo:** es un objeto o aparato electrónico diseñado para cumplir una función específica o desempeñar una tarea determinada.

n) **Emisiones electromagnéticas:** energía radiada en forma de ondas electromagnéticas que se propagan a través del espacio. Estas ondas varían en frecuencia y longitud de onda, abarcando desde las ondas de radio de baja frecuencia hasta los rayos gamma de alta frecuencia.

o) **Equipo de Respuesta a Incidentes de Seguridad Informática:** conjunto multidisciplinario de profesionales especializados, responsable de actuar ante la ocurrencia de un incidente cibernético o ciberataque, con el propósito de contenerlo, mitigar sus efectos y coordinar las acciones necesarias para la recuperación y fortalecimiento de la resiliencia de los sistemas afectados.

p) **Espectro electromagnético:** rango completo de todas las longitudes de onda de radiación electromagnética, que incluye desde ondas de radio de baja frecuencia hasta rayos gamma de alta frecuencia.

q) **Evidencia digital:** es todo indicio correspondiente a un registro de información guardada o difundida a través de un sistema informático y sistemas que utilice tecnologías de la información y la comunicación, que puede utilizarse como prueba en un proceso judicial.

r) **Incidente**: un acontecimiento actual o potencial que resultará en consecuencias adversas a un sistema informático o la información que un sistema procese, guarde o transmita y que requiera de una respuesta para mitigar las consecuencias.

s) **Incidente cibernético:** es un evento que afecta la ciberseguridad de un sistema informático o la información que un sistema procesa, guarda o transmite; o cualquier resultado de una actividad maliciosa o no.

t) **Infraestructura crítica:** son las infraestructuras físicas o digitales, públicas o privadas, que por su tipo de servicio son indispensables y no permiten soluciones alternativas; por lo que su amenaza, ataque, destrucción o bloqueo, tendría un grave impacto sobre los servicios esenciales, seguridad, economía y finanzas del país.

u) **Integridad:** atributo de la información que asegura su exactitud, consistencia y veracidad, evitando modificaciones no autorizadas, pérdidas o alteraciones, tanto durante su almacenamiento como en su transmisión o procesamiento.

v) **Prestador de servicios:** cualquier persona física o jurídica que ofrezca una actividad de servicio a otra persona física o jurídica, relacionado a las tecnologías de la información y la comunicación.

w) **Programa informático:** conjunto de instrucciones o código escrito en un lenguaje de programación que permite a una computadora realizar tareas específicas.

x) **Proveedor de servicios:** son todas aquellas entidades públicas o privadas que ofrecen sus servicios a los usuarios, con la posibilidad de comunicarse a través de un sistema informático. Asimismo, cualquier otra entidad que procese o almacene datos informáticos para ese servicio de comunicación o sus usuarios.

y) **Resiliencia:** capacidad de los sistemas, infraestructuras, servicios y organizaciones para anticipar, resistir, adaptarse y recuperarse eficazmente frente a cualquier tipo de incidente que afecte la seguridad de la información, garantizando la continuidad de las operaciones, la protección de los datos y la funcionalidad de las aplicaciones.

z) **Sistema informático:** conjunto de uno o más dispositivos electrónicos, interconectados o independientes, cuya función principal, o la de alguno de sus componentes, es el tratamiento automatizado de datos mediante la ejecución de programas informáticos. Incluyen tanto el hardware como el software necesario para el procesamiento, almacenamiento y transmisión de información digital.

aa) **Vulnerabilidad cibernética:** debilidad, deficiencia o falla presente en uno o más activos de información, sistemas informáticos, redes de telecomunicaciones o controles de seguridad dentro del ciberespacio, que puede ser aprovechada por una ciberamenaza para comprometer la confidencialidad, integridad, disponibilidad o autenticidad de la información, causando daño o impacto adverso.

TÍTULO II

CIBERDELITOS

CAPÍTULO I

DELITOS CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS O SISTEMAS QUE UTILICEN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 5. Acceso ilícito. Comete el delito de acceso ilícito, quien accediere sin autorización, por cualquier método, a todo o parte de un sistema informático o sistema que utilice tecnologías de la información y la comunicación, en cualquiera de los casos siguientes:

a) Cuando el acceso se realice infringiendo medidas de seguridad; o,
b) Cuando el acceso se realice con la intención de obtener datos informáticos o causar un perjuicio específico.

Al responsable de este delito se le impondrá una pena de prisión de 5 a 8 años.

La pena será de 8 a 10 años en cualquiera de los siguientes casos:

a) Cuando el hecho sea cometido por empleado o funcionario público;
b) Cuando resulte en pérdidas económicas que interfieran o ataquen a la integridad, confidencialidad, disponibilidad, de los sistemas informáticos que afecten servicios esenciales o infraestructuras críticas;
c) Cuando del hecho se apodere de información o haga uso de la misma;
d) Cuando de la acción realizada resulte supresión o la modificación de datos confidenciales, reservados o de seguridad nacional.

Artículo 6. Interceptación ilícita. Comete el delito de interceptación ilícita quien, sin autorización y por cualquier medio o forma, intercepte datos informáticos en transmisiones en un sistema informático, que utilice tecnologías de la información y la comunicación u otras, incluidas las emisiones electromagnéticas provenientes o efectuadas dentro del

mismo, que transporte dichos datos informáticos. Al responsable de este delito se le impondrá una pena de prisión de 6 a 8 años.

La pena será de 8 a 10 años en cualquiera de los siguientes casos:

a) Cuando el hecho sea realizado por cualquier persona que preste o haya prestado sus servicios, directa o indirectamente a la persona individual o jurídica afectada;
b) Cuando resulte en pérdidas económicas que interfieran o ataquen a la integridad, confidencialidad, disponibilidad, de los sistemas informáticos que afecten servicios esenciales o infraestructuras críticas;
c) Cuando de la comisión del delito resulte en daño patrimonial de las personas individuales y jurídicas;
d) Cuando del hecho se apodere de información o haga uso de la misma.

Artículo 7. Ataque a la integridad de los datos informáticos. Comete el delito de ataque a la integridad de los datos informáticos quien, sin autorización, oculte, dañe, borre, deteriore, altere o suprima datos o registros informáticos; al responsable se le impondrá una pena de prisión de 6 a 10 años.

La pena será de 10 a 12 años en cualquiera de los siguientes casos:

a) Cuando el hecho sea realizado por cualquier persona que preste o haya prestado sus servicios, directa o indirectamente a la persona individual o jurídica afectada;
b) Cuando se cometa este delito a datos informáticos relacionados con: actividades comerciales, financieras, activos o pasivos bancarios, con los estados contables o situación patrimonial de personas físicas o jurídicas;
c) Cuando resulte en pérdidas económicas que interfieran o ataquen a la integridad, confidencialidad, disponibilidad, de los sistemas informáticos que afecten servicios esenciales o infraestructuras críticas;
d) Cuando el hecho sea cometido por empleado o funcionario público;
e) Cuando del hecho se apodere de información o haga uso de la misma;
f) Cuando de la acción realizada resulte supresión o la modificación de datos confidenciales, reservados o de seguridad nacional.

Artículo 8. Ataque a la integridad del sistema informático. Comete el delito de ataque a la integridad del sistema informático quien, sin autorización, ataque, degrade, interrumpa, obstaculice o perturbe el funcionamiento normal de un sistema informático o sistemas que utilicen tecnologías de la información y la comunicación, por cualquier medio, al responsable de este delito se le impondrá una pena de prisión de 6 a 8 años.

La pena será de 8 a 10 años en cualquiera de los siguientes casos:

a) Cuando el hecho sea realizado por cualquier persona que preste o haya prestado sus servicios, directa o indirectamente a la persona individual o jurídica afectada;

b) Cuando se cometa este delito a datos informáticos relacionados con: actividades comerciales, financieras, activos o pasivos bancarios, con los estados contables o situación patrimonial de personas físicas o jurídicas;
c) Cuando el hecho sea cometido por empleado o funcionario público;
d) Cuando del hecho se apodere de información o haga uso de la misma.

Cuando resulte en pérdidas económicas que interfieran o ataquen a la integridad, confidencialidad, disponibilidad, de los sistemas informáticos que afecten servicios esenciales, infraestructuras críticas o seguridad nacional la pena será hasta 30 años de prisión.

CAPÍTULO II

DELITOS INFORMÁTICOS

Artículo 9. Falsificación informática. Comete el delito de falsificación informática quien sin autorización introduzca, altere, borre o suprima datos o registros informáticos, que se encuentren en un sistema informático o sistema que utilice tecnologías de la información y la comunicación, quien genere datos no auténticos para que sean tomados o utilizados como auténticos, con independencia de que los datos sean legibles e inteligibles directamente, al responsable de este delito se le impondrá una pena de prisión de 6 a 8 años.

La pena será de 8 a 10 años en cualquiera de los siguientes casos:

a) Cuando el hecho sea realizado por cualquier persona que preste o haya prestado sus servicios, directa o indirectamente a la persona individual o jurídica afectada;
b) Cuando se cometa este delito a datos informáticos relacionados con: actividades comerciales, financieras, activos o pasivos bancarios, con los estados contables o situación patrimonial de personas físicas o jurídicas;
c) Cuando el hecho sea cometido por empleado o funcionario público;
d) Cuando del hecho se apodere de información o haga uso de la misma.

Cuando resulte en pérdidas económicas que interfieran o ataquen a la integridad, confidencialidad, disponibilidad, de los sistemas informáticos que afecten servicios esenciales, infraestructuras críticas o la seguridad nacional la pena será hasta 30 años de prisión.

Artículo 10. Apropiación de identidad ajena. Comete el delito de apropiación de identidad ajena, quien, sin autorización, utilizando cualquier forma, medio o técnicas de ingeniería social, ejecute cualquiera de las acciones siguientes: usurpe, falsifique, adopte o suplante, la identidad de otra persona individual o jurídica, a través de un sistema informático o sistema que haga uso de tecnologías de la información y la comunicación, al responsable de este delito se le impondrá una pena de prisión de 6 a 8 años.

La pena será de 8 a 10 años en cualquiera de los siguientes casos:

a) Cuando se cometa este delito a datos informáticos relacionados con: actividades comerciales, financieras, activos o pasivos bancarios, con los estados contables o situación patrimonial de personas físicas o jurídicas;
b) Cuando resulte en pérdidas económicas que interfieran o ataquen a la integridad, confidencialidad, disponibilidad, de los sistemas informáticos que afecten servicios esenciales o infraestructuras críticas;
c) Cuando el hecho sea cometido por empleado o funcionario público;
d) Cuando del hecho se apodere de información o haga uso de la misma.

Artículo 11. Fraude informático. Comete el delito de fraude informático, quien, sin autorización, para obtener algún beneficio para sí mismo o para otras personas, mediante error, ardid, engaño o cualquier acción delictiva, incluyendo uso de ingeniería social o manipulación de un sistema que utilice tecnologías de la información y la comunicación o de sus componentes, produciendo daño, perjuicio o defraudación en su patrimonio, mediante:

a) La introducción, alteración, borrado o supresión de datos informáticos; o
b) Cualquier interferencia en el funcionamiento de un sistema informático.

La pena será de 8 a 10 años en cualquiera de los siguientes casos:

a) Cuando se cometa este delito a datos informáticos relacionados con: actividades comerciales, financieras, activos o pasivos bancarios, con los estados contables o situación patrimonial de personas físicas o jurídicas;
b) Cuando resulte en pérdidas económicas que interfieran o ataquen a la integridad, confidencialidad, disponibilidad, de los sistemas informáticos que afecten servicios esenciales o infraestructuras críticas;
c) Cuando el hecho sea cometido por propietario de empresa o negocio, socio de cualquier sociedad, cooperativista, directivo, empleado o funcionario público;
d) Cuando del hecho se apodere de información o haga uso de la misma;
e) Cuando el hecho sea realizado por cualquier persona que preste o haya prestado sus servicios, directa o indirectamente a la persona individual o jurídica afectada.

Artículo 12. Abuso de dispositivos. Comete el delito de abuso de dispositivos, quien, sin autorización, realice cualquiera de los actos siguientes:

a) Produzca, venda, obtenga para su utilización, posea, importe, difunda o de cualquier otra forma ponga a disposición:
    a) Cualquier dispositivo, programa informático, aplicaciones o sistema informático, o la combinación de estos, concebidos o adaptados principalmente para la comisión de cualquiera de los delitos previstos en los artículos del 5 al 11 de la presente Ley; o,
    b) Contraseñas, códigos de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático o sistema que

utilice tecnologías de la información y la comunicación, con el objeto de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos del 5 al 11 de la presente ley; o,

b) Cree, utilice, altere, capture, grabe, copie o transfiera de un dispositivo a otro o cualquier instrumento destinado a los mismos fines, los códigos de identificación y acceso al servicio o sistema informático o sistema que utilice tecnologías de la información y la comunicación, que permita la operación paralela, simultanea o independiente de un servicio o sistema informático o sistema que utilice tecnologías de la información y la comunicación, legítimamente obtenido por un tercero; o bien, con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos del 5 al 11 de la presente ley.

Al responsable de este delito se le impondrá una pena de prisión de 6 a 8 años.

La pena será de 8 a 10 años en cualquiera de los siguientes casos:

a) Cuando se cometa este delito a datos informáticos relacionados con: actividades comerciales, financieras, activos o pasivos bancarios, con los estados contables o situación patrimonial de personas físicas o jurídicas;
b) Cuando resulte en pérdidas económicas que interfieran o ataquen a la integridad, confidencialidad, disponibilidad, de los sistemas informáticos que afecten servicios esenciales o infraestructuras críticas;
c) Cuando el hecho sea cometido por empleado o funcionario público;
d) Cuando del hecho se apodere de información o haga uso de la misma.

Artículo 13. Delitos de la propiedad intelectual, derechos de autor, propiedad industrial y delitos informáticos. Cuando los delitos establecidos en el Decreto Número 57-2000 del Congreso de la República de Guatemala, Ley de Propiedad Industrial; el Decreto Número 33-98 del Congreso de la República de Guatemala, Ley de Derechos de Autor y Derechos Conexos; y, los contenidos en el Título VI, Capítulo VII del Decreto 17-73 del Congreso de la República de Guatemala, Código Penal, se cometan a escala comercial y por medio de un sistema informático o tecnologías de la información y la comunicación, a los responsables de dichas conductas se les aumentará la pena en una cuarta parte.

Artículo 14. Pornografía infantil. Cuando mediante el uso de sistemas informáticos o tecnologías de la información y la comunicación, se cometan los delitos tipificados en los artículos 173 bis, 174, 188, 189, 190, 192, 195 bis, 195 ter, 196 del Decreto 17-73 del Congreso de la República de Guatemala, las penas a los responsables se aumentarán de conformidad con lo establecido en el artículo 195 Quinquies, del Decreto 17-73 del Congreso de la República de Guatemala, Código Penal.

Artículo 15. Uso ilegal de bloqueadores o inhibidores de señal. Comete el delito de uso ilegal de bloqueadores o inhibidores de señal quien utilice u opere equipos que bloqueen, cancelen o anulen las señales de telefonía celular, radiocomunicación o transmisión de

datos o imagen, para cometer acciones ilícitas, al responsable de este delito se le impondrá una pena de prisión de 6 a 10 años.

CAPÍTULO III

RESPONSABILIDAD Y PENAS ACCESORIAS

Artículo 16. Responsabilidad de las personas individuales y penas accesorias. Las sanciones penales establecidas en la presente ley se aplicarán sin perjuicio de las responsabilidades civiles o administrativas que correspondan y las contenidas en otras leyes.

Artículo 17. Personas jurídicas. En lo relativo a las personas jurídicas, independientemente de la responsabilidad penal de sus propietarios, directores, gerentes, administradores, funcionarios, empleados o representantes legales, cuando hubieren sido utilizadas para cometer en cualquier forma un hecho ilícito establecido en la presente ley, se le impondrá una multa de Q.100,000.00 a Q.300,000.00; atendiendo a la gravedad y circunstancias en que se cometió el delito. Bajo apercibimiento que en caso de reincidencia se ordenara la cancelación de la personería jurídica en forma definitiva y se le sancionara con:

a) Inmovilización de cuentas bancarias y bienes inmuebles, siempre y cuando se garanticen las prestaciones laborales, según lo determine el órgano jurisdiccional competente;
b) Suspensión de las patentes y permisos que hayan sido debidamente extendidas y que hubieren sido utilizados de cualquier forma para la comisión del hecho delictivo;
c) La exclusión de participar en los procesos de concurso, celebrar contratos y proveedores del Estado, de modo definitivo o por un periodo no menor de cinco años;
d) La prohibición definitiva o por un periodo no menor de cinco años, para participar en actividades destinadas a la captación de títulos valores;
e) Comiso de los bienes o ganancias que se hayan obtenido por la comisión del delito; y,
f) La publicación de la sentencia pronunciada o la difusión de esta, de conformidad con el Decreto Numero 17-73 del Congreso de la República, Código Penal, en el diario escrito y digital de mayor circulación.

TÍTULO III
REGLAS PROCESALES
MEDIDAS CAUTELARES, PROCESALES Y PROCEDIMENTALES

Artículo 18. Acción pública. Los delitos regulados en la presente ley son de Acción Pública.

Artículo 19. Ámbito de aplicación de las disposiciones de procedimiento. Las normas del presente capitulo se aplicarán a:

a) Los delitos previstos en esta ley;
b) Cualquier otro delito cometido por medio de un sistema informático o sistema que utilice tecnologías de la información y la comunicación; y,
c) La obtención de indicios, medios de investigación o pruebas informáticas, digitales o electrónicas de cualquier delito.

Artículo 20. Admisión de la prueba. Los órganos jurisdiccionales admitirán como medios probatorios al proceso, las pruebas digitales que se relacionen con los contenidos de la presente ley, observando en todo momento las disposiciones establecidas en el Decreto 51-92 del Congreso de la República de Guatemala, Código Procesal Penal.

Artículo 21. Valoración de la prueba. Los órganos jurisdiccionales deberán valorar los medios probatorios incorporados al proceso, determinando que hayan sido obtenidos mediante un procedimiento permitido conforme a las disposiciones establecidas en el Decreto 51-92 del Congreso de la República de Guatemala, Código Procesal Penal.

Artículo 22. Diligencias de urgencia para el aseguramiento de datos. Cuando exista peligro en que los datos objeto de una investigación puedan ser alterados o suprimidos, durante la investigación o procesamiento de los delitos tipificados en la presente ley, se procederá de conformidad con lo establecido en el Decreto 51-92 del Congreso de la República de Guatemala, Código Procesal Penal.

Artículo 23. Orden de acceso y envió de datos. En caso de necesidad y razonabilidad comprobada el órgano jurisdiccional competente podrá solicitar las siguientes medidas a los proveedores de servicios de tecnologías de la información y la comunicación de cualquier tipo, tales como:

a) Que comunique, presente, remita o provea acceso de lectura a los datos alojados en un sistema informático o en un dispositivo de almacenamiento informático o digital que este bajo su poder o control y que se vinculen con la investigación de un delito;
b) Entregue datos de los usuarios o abonados o los datos de identificación y facturación de servicios con los que cuente, diferentes de los datos relativos al tráfico o al contenido;
c) Que indique el tipo de servicio de comunicación utilizado, periodo de servicios y lugar de ubicación de los equipos.

La orden podrá contener la indicación de que la medida deberá mantenerse bajo reserva en un plazo de diez días, plazo que podrá prorrogarse a criterio del órgano jurisdiccional a solicitud del Ministerio Público; y con apercibimiento de certificar lo conducente en caso de incumplimiento.

Artículo 24. Diligencias de investigación, registro y respaldo de medios digitales o electrónicos. El Órgano jurisdiccional competente podrá ordenar a requerimiento del Ministerio Público, el registro de un sistema informático o tecnologías de la información y la comunicación, de una parte, de este o de un medio de almacenamiento de datos informáticos, físicos o digitales, electrónicos o de la comunicación, pudiendo realizar las diligencias de investigación correspondiente.

Cuando surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema informático al que se tiene acceso ilícito desde el dispositivo o sistema inicial; el ente investigador podrá extender o ampliar el registro al otro sistema, siempre que medie orden judicial sobre estos dos últimos aspectos.

Artículo 25. Secuestro de evidencias electrónicas o digitales. Los secuestros de evidencias electrónicas o digitales tales como ordenadores, discos duros, servidores y otros medios de almacenamiento digital, así como la obtención de datos almacenados en la nube y el secuestro de activos digitales vinculados a sistemas informáticos y tecnologías de la información y la comunicación, generando y respetando, la cadena de custodia, deberán realizarse por medio de protocolos y procedimientos que garanticen la integridad, disponibilidad y confidencialidad de la información y la comunicación.

Artículo 26. Tratamiento y medidas de seguridad de los datos. En el marco de una investigación penal relativa a ciberdelitos vinculados a la delincuencia organizada, delitos transnacionales o que afecten directa y gravemente infraestructuras críticas o servicios esenciales del Estado, el órgano jurisdiccional competente, a solicitud del Ministerio Público y mediante resolución debidamente motivada, podrá autorizar, de manera excepcional y limitada, las medidas siguientes:

a) La interrupción temporal de transmisiones de datos informáticos que representen una amenaza inminente y grave contra sistemas, servicios esenciales o infraestructuras críticas, siempre que la medida sea estrictamente necesaria, idónea y proporcional al fin legítimo perseguido.
b) La interceptación, grabación y reproducción de comunicaciones informáticas o similares, incluyendo aquellas realizadas a través de sistemas informáticos y tecnologías de la información y la comunicación, únicamente cuando existan indicios fundados y objetivos de que resultarán imprescindibles para el esclarecimiento de los hechos investigados.

La resolución judicial deberá señalar expresamente: el alcance de la medida, los sistemas o dispositivos a intervenir, el motivo de su necesidad, así como el plazo de duración, que no podrá exceder de dos meses, prorrogable por una sola vez y por igual período, siempre que subsistan las causas que la motivaron y se justifique nuevamente su necesidad.

En todo caso, la ejecución de estas medidas deberá garantizar la protección de los derechos fundamentales reconocidos en la Constitución Política de la República, en

particular la inviolabilidad de las comunicaciones privadas y la protección de datos personales, siendo nula de pleno derecho cualquier autorización que se aparte de los límites aquí previstos.

Para el caso de interceptaciones, se aplicarán supletoriamente las disposiciones del Titulo Tercero, Capitulo Tercero del Decreto Número 21-2006 del Congreso de la República, Ley contra la Delincuencia Organizada.

Artículo 27. Comiso. El órgano jurisdiccional competente podrá ordenar el comiso de los objetos o instrumentos del delito, debiendo observarse lo regulado en el Decreto Numero 17-73 del Congreso de la Republica de Guatemala, Código Penal; Decreto Numero 51-92 del Congreso de la Republica de Guatemala, Código Procesal Penal; Decreto Numero 21-2006 del Congreso de la Republica de Guatemala, Ley Contra Delincuencia Organizada; y, Decreto 67-2001 del Congreso de la República de Guatemala, Ley Contra Lavado de Dinero u Otros Activos.

TITULO IV

GESTIÓN Y VIGILANCIA DE LA CIBERSEGURIDAD

CAPITULO ÚNICO

CENTROS DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

Artículo 28. Creación del Centro de Respuesta a Incidentes de Seguridad Informática de Guatemala. Se crea el Centro de Respuesta a Incidentes de Seguridad Informática de Guatemala, en adelante conocido como CSIRT-GT, es el órgano técnico del Consejo Nacional de Seguridad, responsable del análisis, gestión, coordinación y respuesta ante un incidente cibernético o ciberataque, de ciberseguridad a nivel nacional.

Artículo 29. Funciones del CSIRT-GT. Las funciones del CSIRT-GT son:

a) Monitoreo permanente para la atención de incidentes cibernéticos y ciberataques;
b) Asegurar la continuidad operativa y rendimiento de la red y sistemas de las infraestructuras críticas a nivel nacional;
c) Prestar servicios proactivos de ciberseguridad;
d) Prestar servicios reactivos de ciberseguridad;
e) Prestar servicios post incidentes cibernéticos y ciberataques;
f) Detectar, investigar y mitigar incidentes cibernéticos y ciberataques;
g) Coordinar con los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT´s) internacionales, sectoriales e institucionales;
h) Dar respuesta a incidentes cibernéticos y ciberataques que atenten contra la integridad, confidencialidad y disponibilidad de los sistemas que hagan uso de tecnologías de la información y comunicación a nivel nacional;

i) Rendir informes periódicos y específicos al Consejo Nacional de Seguridad, sobre la atención, seguimiento y resolución de ciberataques e incidentes cibernéticos gestionados;
j) Establecer y actualizar los procedimientos para la prevención, detección, análisis, contención, mitigación y recuperación de ciberataques e incidentes cibernéticos;
k) Identificar, clasificar, analizar y evaluar la gravedad de ciberataques e incidentes cibernéticos a nivel nacional;
l) Emitir alertas e informar oportunamente a los potenciales afectados de ciberataques e incidentes cibernéticos;
m) Colaborar con los procesos continuos de auditoría de ciberseguridad en las instituciones del Estado, garantizando la identificación, prevención, protección, detección, preparación, recuperación y respuesta de vulnerabilidades;
n) Elaborar informes, coordinar y dar seguimiento en los casos atendidos; brindando asistencia técnica, según corresponda;
o) Realizar ejercicios y simulacros para la atención de ciberataques e incidentes cibernéticos;
p) Elaborar el Código de Ética para los actores involucrados en la ciberseguridad; y,
q) Otras que de acuerdo con la evolución de la ciberseguridad y el reglamento correspondientes sean necesarias.

Artículo 30. Director General del CSIRT-GT. El Director General del CSIRT-GT, será nombrado por el Presidente de la República, de una terna propuesta por el Consejo Nacional de Seguridad, mediante un proceso de selección técnico, transparente y competitivo, que garantice la idoneidad profesional, la capacidad técnica y la integridad ética del candidato.

El Director General podrá ser removido por el Presidente de la República, por causa justificada, con conocimiento del Consejo Nacional de Seguridad.
El período de funciones del Director General será de seis años, el cual podrá ser reelegido.

El proceso de selección deberá regirse por criterios objetivos, considerando como mínimo los siguientes aspectos:

a) Formación académica de nivel universitario en carreras afines, y grado mínimo de maestría en áreas como seguridad nacional, ciberseguridad, sistemas informáticos y tecnologías de la información y la telecomunicación, gestión de riesgos o disciplinas relacionadas;
b) Certificaciones vigentes y actualizadas en materia de ciberseguridad o relacionadas, y reconocidas en las buenas prácticas de la industria;
c) Experiencia comprobable mínima de cinco (5) años en la gestión, dirección o coordinación en materia de ciberseguridad en el sector público o privado;
d) Conocimiento profundo de los marcos regulatorios nacionales e internacionales en materia de ciberseguridad, continuidad operativa, ciberresiliencia y gestión de crisis;

e) Capacidad demostrable de coordinación interinstitucional y liderazgo en entornos multidisciplinarios o multisectoriales; y,
f) Formación en idioma inglés, comprobable.

Artículo 31. Jerarquía de los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT´s). Para un mejor entendimiento, se establece la siguiente jerarquía y organización de los Centros de Respuesta a Incidentes de Seguridad Informática

a) **CSIRT-GT:** es el ente rector de los CSIRT's con objeto y funciones establecidas en esta Ley, sin limitación alguna de brindar apoyo a solicitud de los Centros de Respuesta a Incidentes, así como al Ministerio Público.
b) **CSIRT-Sectoriales:** son instancias de creación obligatoria que integrarán a los CSIRT´s por sectores estratégicos, quienes deberán contar con un CSIRT y con un Oficial de Seguridad de la Información, ambos independientes del área de informática. Su función principal es brindar atención primaria a los ciberataques e incidentes cibernéticos de su sector y reportarlos al CSIRT-GT dentro del plazo que establezca la normativa.
   Los sectores estratégicos de los CSIRT-Sectoriales, se identifican, más no se limitan a los siguientes: Sector Gobierno y Administración Pública; Sector Químico; Sector Hídrico; Sector Energético; Sector Salud; Sector Tecnologías de la Información y la Comunicación (TIC); Sector Transporte; Sector Alimentario; Sector Tributario; Sector Financiero; Sector Económico; Sector Turístico; y Sector Privado.
c) **CSIRT-Institucionales:** son entidades, públicas y privadas, que cuenten con sistemas de información que almacenen, compartan o actualicen información de los ciudadanos o de carácter estratégico del Estado; deberán contar con un CSIRT y con un Oficial de Seguridad de la Información, ambos independientes del área de informática, siendo responsables de la primera respuesta ante ciberataques e incidentes cibernéticos.
   Si el ciberataque e incidentes cibernéticos superan sus capacidades de respuesta, deben elevarlo a la instancia superior; si el ciberataque e incidentes cibernéticos son de grandes dimensiones y ponen en riesgo la infraestructura crítica o la continuidad de servicios esenciales para la población, deberán dirigirlo directa y obligatoriamente al CSIRT-GT.

Las municipalidades y aquellas instituciones que conforman el sector privado que operan o administran infraestructuras críticas que lo requieran, deberán contar con un CSIRT y con un Oficial de Seguridad de la Información, ambos independientes del área de informática.

Los CSIRT´s deberán de implementar mecanismos de anonimización en los reportes de ciberataques e incidentes cibernéticos, para garantizar la confidencialidad, integridad y disponibilidad de la información, datos personales e institucionales, en lo público y privado.

Todos los CSIRT´s tienen la obligación de reportar, en un período no mayor a los 30 minutos, y de forma anónima resguardando la confidencialidad de las instituciones públicas y privadas que sean afectadas por ciberataques e incidentes cibernéticos, al CSIRT-GT.

Artículo 32. Oficial de Seguridad de la Información. Las entidades públicas y privadas que creen un CSIRT, deberán nombrar un Oficial de Seguridad de la información, que será el enlace con el CSIRT-GT y CSIRT-sectorial.

Se deberá elaborar el reglamento correspondiente para la descripción de las funciones.

TITULO V

CIBERDEFENSA
CAPÍTULO ÚNICO

Artículo 33. Las funciones para la Ciberdefensa. El Ministerio de la Defensa Nacional establecerá permanentemente las acciones para la ciberdefensa, en función de:

a) Dar protección preventiva y activa de redes militares y sistemas informáticos y tecnologías de la información y la comunicación que integren las infraestructuras críticas que atenten contra la Defensa Nacional;
b) Desarrollar acciones defensivas y ofensivas para la protección de las infraestructuras críticas que atenten contra la Defensa Nacional, conforme lo determine el Consejo Nacional de Seguridad, presidido por el Presidente de la República;
c) Planificar, identificar, recolectar, procesar, analizar, producir, distribuir y difundir información de manera oportuna para la ciberdefensa, estableciendo los protocolos necesarios;
d) Dar apoyo a las operaciones militares de tierra, aire y mar;
e) Mantener comunicación y coordinación permanente con el CSIRT-GT;
f) Coordinar con los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT´s) internacionales, sectoriales e institucionales, públicos y privados, en aquellos casos que se afecte las infraestructuras críticas, conforme lo determine el Presidente de la República en Consejo Nacional de Seguridad;
g) Dar apoyo al CSIRT-GT en aquellos casos en que sus capacidades técnicas u operativas sean sobrepasadas, conforme lo determine el Consejo Nacional de Seguridad, presidido por el Presidente de la República;
h) Ser el punto de contacto a nivel internacional en materia de ciberdefensa, para brindar seguimiento, apoyo y recomendaciones, cuando le sea requerido;
i) Crear los marcos normativos y la doctrina para la ciberdefensa;
j) Establecer y actualizar, los protocolos y estándares, para la prevención, detección, contención, protección, recuperación de los sistemas y respuesta del Ministerio de la Defensa Nacional;
k) Diseñar y realizar programas de formación continua, entrenamiento especializado, simulacros técnicos y ejercicios conjuntos en materia de ciberdefensa, a nivel nacional e internacional;

l) Rendir informes al Consejo Nacional de Seguridad, mensualmente o cuando sean necesarios, sobre la atención, seguimiento y resolución de los incidentes gestionados para la ciberdefensa; y,
m) Asesorar técnicamente en el diseño de políticas, estrategias, programas y acciones en materia de ciberdefensa.

TÍTULO VI
FORTALECIMIENTO INSTITUCIONAL Y COOPERACIÓN INTERNACIONAL
CAPÍTULO I

RED DE ATENCIÓN PERMANENTE 24/7 GUATEMALA.

Artículo 34. Red de Asistencia Mutua Contra Delitos informáticos (RED 24/7 Guatemala). El Ministerio Público creara una unidad de atención permanente, como punto de contacto localizable las veinticuatro horas del dia y siete días a la semana, integrándose a través de redes a las que Guatemala se adhiera o forme parte; la que se denominara Red de Asistencia Mutua Contra Delitos informáticos o RED 24/7 Guatemala; con el objeto de garantizar la prestación de ayuda inmediata a nivel internacional para los fines de las investigaciones o procedimientos relacionados con los indicios de los delitos vinculados a sistemas y datos informáticos, o para la obtención de indicios, medios de investigación o pruebas electrónicas en la comisión de un hecho delictivo. Incluirá los actos que tiendan a facilitar las medidas de conformidad con la legislación nacional y lo establecido en la presente ley.

Artículo 35. Personal especializado. El Ministerio Público deberá contratar y capacitar a personal especializado en ciberseguridad y delitos informáticos para garantizar una respuesta técnica y eficiente ante las solicitudes nacionales e internacionales de cooperación que deba de atender la Red 24/7 Guatemala.

CAPÍTULO II

FORTALECIMIENTO INSTITUCIONAL

Artículo 36. Fortalecimiento del Ministerio Publico en materia de Ciberseguridad. Para el cumplimiento de las disposiciones contenidas en la presente ley, el Ministerio Público deberá crear la Fiscalía Especializada para la investigación de los delitos contenidos en esta ley, con los recursos presupuestarios, físicos, materiales, científicos y humanos que le permitan el cumplimiento de los fines de la misma.

Asimismo, creará la Unidad que lleve el control y registro actualizado de las personas que, en sentencia firme y ejecutoriada, hubieren sido condenadas por los delitos contenidos en la presente ley. El registro deberá contener la siguiente información:

a) Nombre y apellidos y en caso de poseerlos, también se consignarán los correspondientes apodos, seudónimos, sobrenombres o alias;
b) Fotografía;

c) Fecha y lugar de nacimiento;
d) Nacionalidad;
e) Código único de identificación del documento personal de identificación o pasaporte en el caso de personas extranjeras; y,
f) Dirección en la que reside.

Para tal efecto, el Ministerio Público deberá elaborar el proceso correspondiente.

Artículo 37. Fortalecimiento del Instituto Nacional de Ciencias Forenses. Para el cumplimiento de las disposiciones contenidas en la presente ley, el Instituto Nacional de Ciencias Forenses deberá crear una unidad especializada para la investigación científica forense de los delitos contenidos en esta ley, con los recursos presupuestarios, físicos, materiales, científicos y humanos que le permitan el cumplimiento de los fines de la misma.

Artículo 38. Creación de los órganos jurisdiccionales especializados. Corresponde al Estado de Guatemala, a través del Organismo Judicial, garantizar que la aplicación de la presente ley esté a cargo de órganos jurisdiccionales especializados. Para tal efecto, la Presidencia del Organismo Judicial, por medio de la unidad administrativa correspondiente, deberá impulsar la creación y dotación del soporte logístico y técnico necesario para el funcionamiento efectivo de dichos órganos especializados, quienes conocerán en forma exclusiva de los delitos tipificados en esta ley.

En tanto se lleve a cabo dicha implementación, los órganos jurisdiccionales ordinarios continuarán conociendo de las causas relacionadas, conforme a su competencia y jurisdicción.

Artículo 39. Fortalecimiento de la Policía Nacional Civil. Para el cumplimiento de las disposiciones contenidas en la presente ley, la Policía Nacional Civil deberá crear la Dirección de Ciberseguridad y Ciberdelincuencia en temas de ciberdelitos, con los recursos presupuestarios, físicos, materiales, científicos y humanos que le permitan el cumplimiento de los fines de la misma.

Artículo 40. Fortalecimiento del Instituto de la Defensa Publica Penal. Para el cumplimiento de las disposiciones contenidas en la presente ley, el Instituto Nacional de la Defensa Pública Penal deberá contar con profesionales del derecho especializados en ciberdelitos con los recursos presupuestarios, físicos, materiales, científicos y humanos que le permitan el cumplimiento de los fines de la misma.

Artículo 41. Otras acciones de fortalecimiento. Con el propósito de desarrollar y actualizar las normativas vigentes en materia de ciberseguridad, el Estado de Guatemala, por medio de las instituciones competentes, buscara armonizar sus planes con políticas regionales en materia de legislación contra delitos que afecten el uso de las tecnologías de la información y la comunicación, a través de tratados y convenios de forma bilateral o multilateral, para lograr la cooperación técnica y económica internacional, con el fin de

fortalecer los programas de prevención e investigación; y, contrarrestar las conductas antijurídicas reguladas en esta ley.

CAPÍTULO III

COOPERACIÓN INTERNACIONAL

Artículo 42. Cooperación en materia de extradición. Los delitos contemplados en la presente ley darán lugar a la extradición activa o pasiva, de conformidad con la legislación vigente y tratados internacionales de los que Guatemala sea parte.

Artículo 43. Cooperación internacional. En caso de requerimiento de información de carácter internacional, las solicitudes de aseguramiento de datos, solicitudes de presentación de datos, de obtención o confiscación, de acceso libre a datos de fuente abierta y asistencia mutua para obtención de datos sobre el tráfico e interceptación de comunicaciones, se estará a lo dispuesto en tratados y convenios aceptados y ratificados por el Estado de Guatemala, así como al derecho interno.

En caso de orden de aseguramiento de datos informáticos almacenados, solo está permitido que las autoridades competentes ordenen la conservación de los datos, pero no su revelación y en caso de requerimiento de presentación de datos informáticos almacenados en cumplimiento de una orden de presentación si se ordenara su revelación para fines de la investigación, debiendo ser justificado por el Ministerio Publico ante el órgano jurisdiccional competente, quien emitirá la resolución que en derecho correspondiente.

TÍTULO VII

DISPOSICIONES FINALES Y TRANSITORIAS

Artículo 44. Reglamento. El Organismo Ejecutivo deberá elaborar los reglamentos de la presente ley dentro del improrrogable plazo de ciento veinte días a partir de que la misma cobre vigencia.

Por su parte, las entidades gestoras de ciberseguridad deberán adecuarse a las disposiciones de la presente ley, incluyendo la elaboración y aprobación de los manuales, protocolos o reformas a los mismos que sean necesarios para el cumplimiento de sus funciones establecidas en este cuerpo normativo.

Artículo 45. Presupuesto del CSIRT-GT. El Ministerio de Finanzas Públicas debe de asignar una partida presupuestaria especifica para el CSIRT-GT, sujeto a los controles que establece la Constitución Política de la República de Guatemala.

Artículo 46. Presupuesto para la ciberseguridad y ciberdefensa. Las instituciones del Estado mencionadas en esta ley deberán incluir cada año, en su planificación anual de compras y en su anteproyecto de presupuesto, los recursos necesarios para cumplir con las funciones que les asigna esta norma.

En caso de no contar con la asignación presupuestaria suficiente, deberán realizar los ajustes necesarios dentro de su propio presupuesto, con el fin de asegurar la disponibilidad de fondos para ejecutar adecuadamente las actividades establecidas en esta ley, conforme a la normativa vigente en materia presupuestaria.

Artículo 47. Compra de Equipo para ciberseguridad y ciberdefensa. Las adquisiciones de bienes, equipos, sistemas o tecnologías destinadas a la Ciberseguridad y Ciberdefensa deberán realizarse bajo reserva, en virtud de su carácter estratégico y por estar vinculadas a la seguridad nacional.

Dichas compras estarán sujetas a los regímenes especiales de contratación establecidos en la legislación aplicable, garantizando la confidencialidad, protección de la información y el interés superior del Estado.

Asimismo, deberán respetar los estándares internacionales y los parámetros técnicos establecidos en la presente ley y su reglamentación, asegurando que los bienes y servicios adquiridos cumplan con los criterios de calidad, interoperabilidad y seguridad reconocidos por la industria.

Artículo 48. Controles democráticos. Los órganos creados están sujetos a los controles democráticos establecidos en el Capítulo VII del Decreto 18-2008 del Congreso de la República de Guatemala, Ley Marco del Sistema Nacional de Seguridad.

Artículo 49. Se adiciona la literal i) al artículo 2 del Decreto Numero 21-2006 del Congreso de la República, Ley Contra la Delincuencia Organizada, el cual queda de la siguiente manera:

> *i) De los contenidos en la Ley de Ciberseguridad: acceso ilícito; intercepción ilícita; ataque a la integridad de los datos informáticos; ataque a la integridad del sistema informático; falsificación informática; apropiación de identidad ajena; fraude informático; y abuso de dispositivos; así como, otros delitos tipificados en la Ley de Ciberseguridad y en demás cuerpos normativos relacionados con la materia.*

Artículo 50. Derogatorias. Se derogan los artículos 274 "A", 274 "B", 274 "C", 274 "E", 274 "F" y 274 "G" del Decreto 17-73 del Congreso de la Republica de Guatemala, Código Penal.

Se derogan todas las disposiciones que se opongan a la presente ley.

Artículo 51. Vigencia. El presente Decreto entrara en vigencia ciento veinte días después de su publicación en el Diario Oficial.

REMÍTASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.

EMITIDO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, EL __ DE __ DEL AÑO DOS MIL VEINTICINCO