CONGRESO DE LA REPÚBLICA DE GUATEMALA

DECRETO NÚMERO 26-2026

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, privados y público-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 una institucionalidad sólida y articulada en materia de ciberseguridad; así como, mecanismos de intercambio de información sobre riesgos y amenazas cibernéticas entre entidades públicas, privadas y público-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:

La siguiente:

LEY MARCO DE CIBERSEGURIDAD

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto. La presente Ley tiene por objeto crear y desarrollar el marco institucional de la ciberseguridad en Guatemala; así como, establecer un régimen sancionatorio de carácter administrativo, generar el marco jurídico penal y procesal penal en materia de ciberseguridad, promover la cooperación internacional y el fortalecimiento de las capacidades técnicas necesarias para el abordaje de la ciberseguridad a nivel nacional.

Artículo 2. Interés nacional. Se declara de interés nacional dirigir los esfuerzos hacia cumplir el objeto y demás disposiciones de la presente Ley.

Artículo 3. Ámbito de aplicación. El ámbito de aplicación de la presente Ley, lo constituye todo el territorio de la República de Guatemala, el ciberespacio y demás ámbitos territoriales y extraterritoriales establecidos en el ordenamiento jurídico vigente que tengan vinculación con la materia objeto de la presente Ley.

En materia penal, su aplicación tendrá efectos sobre 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 produzcan en el extranjero, utilizando medios que se encuentran en el territorio nacional; o,
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.

CAPÍTULO II
PRINCIPIOS Y DEFINICIONES

Artículo 4. Principios. La presente Ley se regirá por los siguientes principios de ciberseguridad:

a) **Confidencialidad:** Principio que busca prevenir el acceso, uso o divulgación de la información por parte de personas no autorizadas, garantizando que únicamente quienes cuenten con la debida autorización puedan acceder a ella;
b) **Cooperación:** Principio que dispone que las entidades deberán colaborar, compartir información y coordinar acciones entre sí para prevenir, investigar o resolver problemas que no pueden abordarse de manera aislada ante incidentes de ciberseguridad y proteger los sistemas y servicios informáticos esenciales;
c) **Disponibilidad:** Principio que garantiza que la información, los sistemas, servicios y datos estén accesibles y sean utilizables, cuando se necesiten, por personas o entidades autorizadas, sin interrupciones indebidas;

d) **Integridad:** Principio que garantiza que la información y los sistemas se mantengan exactos, completos y sin alteraciones no autorizadas, desde su creación hasta su recepción, evitando modificaciones no autorizadas, pérdidas o alteraciones, tanto durante su almacenamiento como en su transmisión o procesamiento;
e) **Proporcionalidad:** Principio que dispone que las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades de la autoridad competente deberán ser necesarias y proporcionales al grado de exposición a los riesgos, y al eventual impacto social y económico;
f) **Resiliencia:** Principio que dispone la capacidad de un sistema, servicio, organización o infraestructura para anticipar, resistir, absorber, recuperarse y adaptarse rápida y eficazmente frente a incidentes, fallos o ataques que afecten la seguridad de la información, garantizando la continuidad de las operaciones, la protección de los datos y la funcionalidad de los sistemas;
g) **Restricciones de uso:** Principio que garantiza que la información y los sistemas solo deben ser utilizados para los fines específicos para los que fueron recolectados o implementados, y únicamente por las personas o entidades autorizadas, evitando su acceso, uso o divulgación indebida;
h) **Seguridad en el ciberespacio:** Principio que dispone la obligación de garantizar un entorno digital seguro mediante medidas que protejan sistemas, redes y datos frente a riesgos, ataques o actividades ilícitas;
i) **Seguridad por diseño:** Principio que exige integrar medidas de seguridad desde el diseño, creación y desarrollo de sistemas o servicios digitales, garantizando que sean seguros desde su origen; y,
j) **Seguridad informática:** Principio que dispone la obligación de proteger sistemas, redes y datos mediante medidas adecuadas que garanticen su confidencialidad, integridad y disponibilidad.

Artículo 5. Definiciones. Además de las definiciones ya contenidas en el ordenamiento jurídico vigente, para los efectos de la presente Ley, se entenderá por:

a) **Centro de Respuesta a Incidentes de Ciberseguridad de Guatemala:** Equipo nacional responsable de la detección, análisis y respuesta a incidentes de ciberseguridad y ciberataques, con el objetivo de minimizar el impacto de ataques y mejorar la resiliencia digital;
b) **Ciberamenaza:** Fuente potencial de perjuicio, externa o interna, al Estado, que se materializa a través del ciberespacio;
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:** Empleo de las capacidades militares ante las amenazas o actos hostiles de naturaleza cibernética, los cuales afectan las infraestructuras críticas, 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, antijurídicas, 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 física o digital 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) **Datos de tráfico:** Datos informáticos relativos a una comunicación realizada mediante un sistema informático, generados por un sistema que forme parte de la cadena de comunicación, que indiquen su origen, destino, itinerario, hora, fecha, tamaño, duración o tipo de servicio subyacente. Los datos de tráfico no comprenden el contenido de las comunicaciones;

j) **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;

k) **Dispositivo:** Objeto o aparato electrónico diseñado para cumplir una función específica o desempeñar una tarea determinada;

l) **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;

m) **Entorno digital:** El entorno digital comprende las tecnologías y servicios de la información y la comunicación (TIC), incluidos Internet, las redes y dispositivos de comunicaciones móviles y fijas, así como los datos y la información que se procesa, almacena o transmite a través de ellos, u otras tecnologías disponibles de acuerdo a la propia evolución de las mismas;

n) **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;

o) **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;

p) **Evidencia digital:** 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;

q) **Incidente cibernético:** 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;

r) **Infraestructura crítica:** Infraestructuras físicas o digitales, públicas, privadas o público-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;

s) **Infraestructura crítica digital:** Conjunto de sistemas informáticos, redes de comunicaciones, tecnologías de la información, tecnologías de operación, sistemas de control industrial, activos digitales y demás componentes tecnológicos indispensables para el funcionamiento de una infraestructura crítica o la prestación de un servicio esencial, cuya afectación, interrupción, alteración, destrucción o indisponibilidad derivada de un incidente cibernético o ciberataque pueda provocar un impacto grave en la continuidad de dichos servicios, la seguridad nacional, la economía, las finanzas, el orden público o el normal funcionamiento del Estado;

t) **Oficial de seguridad de la información:** Persona responsable de planificar, desarrollar, controlar y gestionar las políticas y procedimientos para mejorar la seguridad de la información dentro de una entidad pública o privada. Su labor incluye prevenir y gestionar riesgos, garantizar el cumplimiento normativo y fomentar una cultura de seguridad en todos los niveles de la entidad;

u) **Operador de servicios esenciales:** Persona individual o entidad pública, privada o publico-privada, responsable de la prestación de un servicio esencial cuya continuidad depende de manera significativa de sistemas informáticos, redes o infraestructuras críticas;

v) **Programa informático:** Conjunto de instrucciones o código escrito en un lenguaje de programación que permite a una computadora realizar tareas específicas;

w) **Proveedor de servicios:** Persona física o jurídica que ofrece sus servicios a los usuarios, con la posibilidad de comunicarse a través de un sistema informático. Asimismo, cualquier otra persona o entidad que procese o almacene datos informáticos para ese servicio de comunicación o sus usuarios;

x) **Sector estratégico:** Es el conjunto articulado de diferentes actividades económicas, servicios públicos, sistemas informáticos o sistemas que utilicen tecnologías de la información y comunicación; así como, infraestructuras físicas, por su naturaleza crítica e interdependiente, son fundamentales para el

funcionamiento continuo del Estado, la seguridad nacional, el bienestar social y el desarrollo económico del país;

y) Servicios esenciales: Aquellos servicios cuya afectación puede causar un grave daño a la vida o integridad física de la población o su abastecimiento; a sectores relevantes de las actividades económicas; al normal funcionamiento de la sociedad o administración del Estado; así como, a la seguridad nacional y el orden público, los cuales estarán incluidos en el Catálogo Nacional de Infraestructuras Críticas Digitales;

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; y,

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
MARCO INSTITUCIONAL DE CIBERSEGURIDAD

CAPÍTULO I
JERARQUÍA INSTITUCIONAL

Artículo 6. Jerarquía institucional de la ciberseguridad. La jerarquía institucional de la ciberseguridad será la siguiente:

a) Consejo Nacional de Ciberseguridad, como ente rector nacional de la ciberseguridad;
b) Ministerio de Gobernación, como ente rector sectorial de la ciberseguridad;
c) Dirección Nacional de Ciberseguridad, como órgano técnico-operativo adscrito al Ministerio de Gobernación.

CAPÍTULO II
CONSEJO NACIONAL DE CIBERSEGURIDAD

Artículo 7. Consejo Nacional de Ciberseguridad. Se crea el Consejo Nacional de Ciberseguridad, en adelante el Consejo o CONCIBER, como ente rector para la toma de decisiones estratégicas sobre los asuntos de interés nacional en materia de ciberseguridad. El Consejo no tendrá presupuesto propio y estará conformado de la forma siguiente:

a) Presidente de la República, quien lo presidirá y tomará las decisiones;
b) Ministro de Gobernación;
c) Ministro de Relaciones Exteriores;
d) Ministro de la Defensa Nacional;
e) Ministro de Comunicaciones, Infraestructura y Vivienda;
f) Ministro de Finanzas Públicas;
g) Secretario de Inteligencia Estratégica del Estado; y,
h) Director General de la Dirección Nacional de Ciberseguridad, quien fungirá como secretario del Consejo.

Los integrantes del Consejo formarán parte del mismo, de forma *ad honorem*, durante el tiempo que dure su cargo o nombramiento, según corresponda.

El Consejo se reunirá de manera ordinaria una vez cada mes y de manera extraordinaria cuando se considere necesario, a solicitud de alguno de sus integrantes. La convocatoria a reunión ordinaria o extraordinaria se realizará por instrucciones del presidente de la República, a través del Ministerio de Gobernación.

Las instituciones representadas en el Consejo deberán atender los lineamientos y directrices planteadas por este, respetando el ámbito de su competencia, para coadyuvar en el cumplimiento de las atribuciones y funciones contempladas en la presente Ley.

Artículo 8. Funciones del Consejo Nacional de Ciberseguridad. Son funciones del Consejo Nacional de Ciberseguridad las siguientes:

a) Conocer y tomar las decisiones estratégicas sobre asuntos nacionales en materia de ciberseguridad;
b) Coordinar y supervisar el funcionamiento de las instituciones responsables de la ciberseguridad;
c) Dar seguimiento y supervisar las políticas en materia de ciberseguridad emitidas por el presidente de la República;
d) Aprobar y supervisar el cumplimiento de las estrategias, planes y protocolos, nacionales y sectoriales, así como, de otros instrumentos en materia de ciberseguridad, los que deberán ser de cumplimiento obligatorio para las entidades del Organismo Ejecutivo y se coordinará su implementación con las entidades autónomas, descentralizadas y del sector privado y público-privado;
e) Aprobar los lineamientos de actuación de los niveles de respuesta ante incidentes cibernéticos, de conformidad con la presente Ley;
f) Constituirse en Comité de Crisis, de conformidad con lo que la presente Ley establece sobre los niveles de respuesta ante incidentes cibernéticos;
g) Promover y gestionar acciones, protocolos, estándares y buenas prácticas para la prevención y gestión de los riesgos y amenazas en ciberseguridad;
h) Promover la actualización del marco normativo e institucional aplicable a la ciberseguridad;
i) Promover la cooperación interinstitucional e intersectorial, a nivel nacional e internacional, en materia de ciberseguridad;

j) Generar los mecanismos legales y técnicos que permitan el intercambio de información nacional e internacional en materia de ciberseguridad;
k) Analizar la información generada y las recomendaciones técnicas emitidas por la Mesa Técnica de Ciberseguridad;
l) Emitir recomendaciones a los sectores estratégicos en materia de ciberseguridad;
m) Elaborar y remitir al presidente de la República la terna de candidatos para el cargo de director general y subdirector general de la Dirección;
n) Convocar a los funcionarios y expertos en materia de ciberseguridad, así como, a las entidades de la sociedad civil y la academia que considere necesarios;
o) Requerir información a la Dirección Nacional de Ciberseguridad sobre las acciones y asuntos de su competencia; y,
p) Otras que establezca la presente Ley o que sean desarrolladas en su reglamento.

Artículo 9. Obligatoriedad de cooperación con el Consejo. Las entidades públicas, privadas y público-privadas deberán cooperar con el Consejo, para garantizar el cumplimiento de las funciones de este y el desarrollo de las capacidades en materia de ciberseguridad, facilitando la información pertinente y atendiendo los lineamientos, estrategias y acciones en la materia, de conformidad con la ley.

El deber de cooperación no comprende la entrega de información protegida por el artículo 24 de la Constitución Política de la República de Guatemala, por el artículo 63 del Decreto Número 19-2002 ni por el Decreto Número 15-2026, ambos del Congreso de la República, la cual solo podrá obtenerse por la autoridad, por el canal y con los requisitos previstos en dichas normas o mediante orden de juez competente.

La información que se facilite al Consejo y a la Dirección en cumplimiento de este artículo será agregada o anonimizada, tendrá carácter confidencial o reservado conforme a los artículos 22 y 23 del Decreto Número 57-2008 del Congreso de la República y se requerirá y tratará conforme a los principios de necesidad, proporcionalidad y reserva, sin afectar la relación contractual ni la continuidad de los servicios esenciales.

CAPÍTULO III
DIRECCIÓN NACIONAL DE CIBERSEGURIDAD

Artículo 10. Dirección Nacional de Ciberseguridad. Se crea la Dirección Nacional de Ciberseguridad, en adelante la Dirección o DICIBER, como una dependencia del Ministerio de Gobernación, eminentemente técnico-operativa y especializada a nivel nacional en materia de ciberseguridad.

Debido a la naturaleza y funciones especializadas en materia de ciberseguridad que llevará a cabo la Dirección, esta tendrá presupuesto propio y deberá considerarse como cuerpo de seguridad del Estado.

Su estructura organizacional y demás disposiciones de funcionamiento serán desarrolladas en la presente Ley, en su reglamento y en el reglamento orgánico interno respectivo.

Artículo 11. Funciones de la Dirección. Serán funciones de la Dirección las siguientes:

a) Cumplir con las directrices y coordinación del Consejo, bajo la rectoría sectorial del Ministerio de Gobernación;
b) Elaborar la Política Nacional de Ciberseguridad;
c) Elaborar y presentar al Consejo para su aprobación las estrategias, planes y protocolos, nacionales y sectoriales, en materia de ciberseguridad;
d) Informar periódicamente al Consejo sobre el cumplimiento de sus funciones, acciones y asuntos de su competencia, especialmente, en relación a la atención, seguimiento y resolución de incidentes cibernéticos y ciberataques;
e) Coordinar, presidir y convocar a la Mesa Técnica de Ciberseguridad;
f) Coordinar las acciones preventivas, reactivas y post incidentes relacionadas con la ciberseguridad;
g) Coordinar los centros de respuesta ante incidentes de ciberseguridad a nivel nacional;
h) Coordinar la respuesta inmediata ante incidentes de ciberseguridad o ciberataques a nivel nacional, asegurando la continuidad operativa, rendimiento de la red y sistemas de las infraestructuras críticas digitales;
i) Supervisar las acciones de monitoreo continuo de los sistemas, redes y servicios digitales bajo su ámbito de competencia, así como, la emisión de alertas, boletines y reportes técnicos sobre la materia;
j) Elaborar, actualizar y presentar al Consejo para su aprobación el Protocolo de Actuación de los Niveles de Respuesta ante Incidentes Cibernéticos;
k) Establecer, actualizar y estandarizar los procedimientos para la prevención, detección, análisis, contención, mitigación y recuperación de ciberataques e incidentes cibernéticos;
l) Establecer los estándares y las obligaciones mínimas de cumplimiento de los Equipos de Respuesta ante Incidentes de Ciberseguridad y de los Oficiales de Ciberseguridad;
m) Llevar un registro a nivel nacional de los Centros de Respuesta a Incidentes de Ciberseguridad (CRICs) y de los Oficiales de Ciberseguridad;
n) Velar porque el personal de la Dirección reúna las competencias suficientes y especializadas en materia de su competencia;
o) Coordinar con instituciones competentes, nacionales e internacionales, en la prevención y persecución de ciberdelitos;
p) Coordinar con el Ministerio de la Defensa Nacional los mecanismos de cooperación, intercambio de información, asistencia y apoyo técnico necesarios, para la adecuada articulación entre ciberseguridad y ciberdefensa, respetando las competencias exclusivas de cada institución;
q) Promover alianzas estratégicas para la inversión, la investigación y el desarrollo en materia de su competencia;
r) Promover acciones y programas de formación, capacitación, concientización y prevención en materia de su competencia; y,

s) Otras que de acuerdo con las necesidades de la materia sean establecidas en esta Ley o por la vía reglamentaria.

Artículo 12. Director General de la Dirección Nacional de Ciberseguridad. El director general de la Dirección Nacional de Ciberseguridad, en adelante el director general, tiene a su cargo la administración y representación legal de la Dirección, por lo que le corresponde el ejercicio de las funciones asignadas a dicha dependencia de conformidad con la ley.

El director general desempeñará sus funciones bajo su exclusiva responsabilidad y en estricto apego al ordenamiento jurídico vigente.

Artículo 13. Nombramiento del Director General. El director general será nombrado por el presidente de la República, de una terna propuesta por el Consejo, garantizando su idoneidad profesional, capacidad técnica e integridad ética.

Artículo 14. Terna para optar al cargo de Director General. Para la selección de la terna para optar al cargo de director general, el Consejo deberá velar porque los perfiles seleccionados cumplan los siguientes requisitos:

a) Ser guatemalteco, hallarse en el goce de sus derechos ciudadanos y ser de reconocida honorabilidad;
b) Poseer título universitario de licenciatura en ciberseguridad, sistemas informáticos, tecnologías de la información, telecomunicaciones, o disciplinas afines;
c) Contar con estudios de posgrado en áreas relacionadas con la materia de ciberseguridad o disciplinas afines;
d) Contar con certificación vigente y actualizada en materia de ciberseguridad, reconocida a nivel internacional;
e) Tener conocimiento de marcos regulatorios nacionales e internacionales en materia relacionada a la competencia de la Dirección;
f) Experiencia mínima comprobable de cinco (5) años en materia de ciberseguridad;
g) Cumplir con los demás requisitos establecidos en la Constitución Política de la República de Guatemala y otras leyes aplicables; y,
h) Otros que sean establecidos por la vía reglamentaria.

Artículo 15. Incompatibilidades. El ejercicio del cargo de director general será incompatible con lo siguiente:

a) Haber sido condenado por delito doloso o encontrarse inhabilitado para el ejercicio de funciones públicas;
b) El ejercicio de cualquier otro cargo público remunerado, salvo la docencia universitaria de conformidad con la ley;
c) El desempeño de cargos directivos, administrativos, o la prestación de servicios técnicos, profesionales, consultorías o asesorías en entidades

públicas, privadas o público-privadas, salvo que renuncie a los mismos previo a la toma de posesión del cargo de director general;

d) La participación, directa o indirecta, individual o por medio de terceros, que genere un conflicto de interés en empresas sujetas a supervisión o regulación por la Dirección General;

e) El ejercicio de cargos de dirección o representación en organizaciones políticas o sindicales; y,

f) Otras que sean establecidas por la vía reglamentaria.

Artículo 16. Prohibiciones. Durante el ejercicio del cargo, el director general tiene prohibido lo siguiente:

a) Intervenir en asuntos en los que tenga interés por motivos personales, familiares o profesionales, debiendo excusarse de conocerlos conforme a la ley;

b) Utilizar o compartir información confidencial obtenida en el ejercicio de sus funciones para beneficio propio o de terceros;

c) Aceptar cualquier tipo de dádivas, regalos o beneficios;

d) Ejercer influencia indebida en procesos administrativos o técnicos bajo su cargo; y,

e) Otras que sean establecidas por la vía reglamentaria.

Artículo 17. Subdirector General de la Dirección Nacional de Ciberseguridad. El subdirector general de la Dirección Nacional de Ciberseguridad, en adelante el subdirector general, será nombrado de la misma forma que el director general. Los requisitos, incompatibilidades y prohibiciones serán los mismos establecidos para el director general.

Artículo 18. Mesa Técnica de Ciberseguridad. El director general coordinará la Mesa Técnica de Ciberseguridad, en adelante la Mesa, como un espacio intersectorial de diálogo y asesoría técnica al Consejo, acerca de los asuntos de interés nacional en materia de ciberseguridad.

La Mesa estará integrada por representantes de los sectores estratégicos relacionados con la materia; así como, por representantes de las entidades de la sociedad civil y la academia que el Consejo autorice.

Todos los representantes deberán llenar un perfil eminentemente técnico y especializado en la materia y desempeñar su representación de forma *ad honorem*. Dicha representación no generará relación laboral alguna con el Consejo, el Ministerio de Gobernación ni la Dirección.

La Mesa se reunirá de manera ordinaria una vez al mes y extraordinariamente cuando sea convocada por el director general, y podrá crear submesas en temas de interés específicos relacionadas a la materia de ciberseguridad y ciberdefensa.

Artículo 19. Funciones de la Mesa Técnica de Ciberseguridad. Serán funciones de la Mesa las siguientes:

a) Brindar asesoría técnica al Consejo en los asuntos de interés nacional en materia de ciberseguridad y ciberdefensa;
b) Generar información, opiniones y recomendaciones técnicas al Consejo sobre lineamientos, estrategias y acciones que traten asuntos de interés nacional en la materia;
c) Colaborar con el desarrollo de capacidades técnicas, el fomento de la cultura de ciberseguridad en el país y la generación de espacios de cooperación interinstitucional; y,
d) Otras funciones que establezca el reglamento de la ley o que sean aprobadas por el Consejo.

CAPÍTULO IV
CENTRO DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD DE GUATEMALA (CRIC-GT)

Artículo 20. Centro de Respuesta a Incidentes de Ciberseguridad de Guatemala. Se crea el Centro de Respuesta a Incidentes de Ciberseguridad de Guatemala, en adelante CRIC-GT, como una dependencia de la Dirección Nacional de Ciberseguridad. La misma será eminentemente técnica y especializada en materia de ciberseguridad y se regirá por la presente Ley y su reglamento.

Artículo 21. Funciones del CRIC-GT: Serán funciones del CRIC-GT las siguientes:

a) Asegurar la continuidad operativa y el rendimiento de la red y los sistemas de las infraestructuras críticas digitales a nivel nacional;
b) Realizar el monitoreo continuo de los sistemas, redes y servicios digitales bajo su ámbito de competencia; así como, la emisión de alertas, boletines y reportes técnicos sobre la materia;
c) Prevenir, detectar, analizar, clasificar y gestionar oportunamente incidentes cibernéticos y ciberataques, conforme a los protocolos de respuesta establecidos;
d) Prestar servicios preventivos, reactivos y post incidentes en materia de ciberseguridad y ciberataques;
e) Informar oportunamente a los potenciales afectados de incidentes cibernéticos o ciberataques;
f) Prestar apoyo técnico y coordinar con los Centros de Respuesta a Incidentes de Ciberseguridad (CRICs), nacionales e internacionales, manteniendo activos los mecanismos de comunicación y cooperación entre los mismos;
g) Elaborar informes sobre los casos en los que haya brindando asistencia técnica en materia de su competencia;
h) 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;

i) Realizar ejercicios y simulacros para la atención de incidentes cibernéticos y ciberataques;
j) Proponer a la Dirección mejoras y buenas prácticas en materia de ciberseguridad; y,
k) Otras que de acuerdo con las necesidades de la materia sean establecidas en esta Ley o por vía reglamentaria.

Artículo 22. Director Técnico del CRIC-GT. El director técnico del CRIC-GT, en adelante el director técnico, tiene a su cargo la administración del mismo por lo que le corresponde el ejercicio de las anteriores funciones.

El director técnico desempeñará sus funciones bajo su exclusiva responsabilidad y en estricto apego a la presente Ley y demás normativa legal aplicable.

Artículo 23. Nombramiento del Director Técnico. El director técnico será nombrado por el Director General, mediante un proceso de selección técnico, transparente y competitivo, que garantice la idoneidad profesional, la capacidad técnica y la integridad ética, debiendo regirse por criterios objetivos. Dicho proceso se fundamentará en la garantía de estabilidad institucional y será desarrollado en el reglamento de la presente Ley.

Las incompatibilidades y prohibiciones serán las mismas establecidas en esta Ley para el director general.

Artículo 24. Requisitos para optar al cargo de Director Técnico. Para optar al cargo de director técnico se requiere cumplir con los siguientes requisitos:

a) Ser guatemalteco, hallarse en el goce de sus derechos ciudadanos y ser de reconocida honorabilidad;
b) Poseer título universitario de licenciatura en ciberseguridad, sistemas informáticos, tecnologías de la información, telecomunicaciones, o disciplinas afines;
c) Contar con estudios de posgrado en áreas relacionadas con la materia de ciberseguridad o disciplinas afines;
d) Tener conocimiento de marcos regulatorios nacionales e internacionales en materia relacionada a la competencia del CRIC-GT;
e) Contar con certificación vigente y actualizada en materia de ciberseguridad, reconocida a nivel internacional;
f) Contar con experiencia mínima comprobable de cinco (5) años en materia relacionada a la competencia del CRIC-GT, en el sector público, privado o público-privado;
g) Cumplir con los demás requisitos establecidos en la Constitución Política de la República de Guatemala y otras leyes aplicables; y,
h) Otros que sean establecidos por la vía reglamentaria.

Artículo 25. Causas de remoción del Director Técnico. El director técnico podrá ser removido del cargo, por cualquiera de las causas siguientes:

a) Incumplimiento reiterado de sus funciones, de acuerdo con lo establecido en el reglamento de la presente Ley;
b) Violación a las incompatibilidades o prohibiciones establecidas en la presente Ley;
c) Incapacidad que le impida el ejercicio del cargo;
d) Negligencia grave en el ejercicio de sus funciones;
e) Faltas a la probidad, ética o transparencia en el ejercicio del cargo; y,
f) Otras que sean establecidas por la vía reglamentaria.

Artículo 26. Procedimiento de remoción del Director Técnico. El director técnico podrá ser removido del cargo por el director general, mediante un procedimiento administrativo, objetivo y transparente, que garantice el derecho de defensa y el debido proceso. Dicho procedimiento será desarrollado en el reglamento de la presente Ley y deberá garantizar como mínimo los siguientes aspectos:

a) La apertura de un expediente administrativo debidamente fundamentado;
b) La notificación formal de los cargos al funcionario;
c) La concesión de audiencia para ejercer su derecho de defensa y presentar pruebas;
d) La emisión de resolución motivada por la autoridad competente; y,
e) La posibilidad de impugnación conforme al ordenamiento jurídico vigente.

Artículo 27. Subdirector Técnico de Ciberseguridad. El subdirector técnico de Ciberseguridad, en adelante el subdirector técnico, será nombrado de la misma nómina de postulantes que optaron al cargo de director técnico, y será removido de la misma forma que el director técnico. Los requisitos, incompatibilidades y prohibiciones serán los mismos establecidos en esta Ley para el director técnico.

Artículo 28. Integración del patrimonio y recursos. El patrimonio de la Dirección se constituirá por el conjunto de bienes, derechos y obligaciones de los que sea titular, así como, por los recursos financieros provenientes de:

a) La asignación anual aprobada por el Congreso de la República dentro del Presupuesto General de Ingresos y Egresos del Estado;
b) Los saldos de caja resultantes de la ejecución presupuestaria de cada ejercicio fiscal, derivados del excedente de los ingresos percibidos sobre los egresos devengados;
c) Los bienes muebles, inmuebles e intangibles que se adquieran o se le transfieran bajo cualquier título legal para el cumplimiento de sus fines institucionales;
d) Las subvenciones, donaciones, aportes de cooperación técnica y créditos que otorguen personas jurídicas, entidades nacionales u organismos internacionales, de conformidad con la ley;

e) Los ingresos extraordinarios que perciba derivados de la suscripción de convenios interinstitucionales, tratados internacionales o por disposición de leyes específicas de la materia; y,

f) Los fondos privativos que se recauden del cobro de multas administrativas, de conformidad con la presente Ley.

CAPÍTULO V
CENTROS DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD (CRICs)

Artículo 29. Centros de Respuesta a Incidentes de Ciberseguridad (CRICs). Los Centros de Respuesta a Incidentes de Ciberseguridad, en adelante CRIC o CRICs, son equipos de respuesta a incidentes de seguridad informática, responsables de la detección, análisis y respuesta a incidentes de ciberseguridad y ciberataques, cada uno dentro del ámbito de su competencia y conforme al nivel de respuesta correspondiente, sin que la existencia de capacidades institucionales o sectoriales implique duplicidad, sustitución o transferencia de las competencias atribuidas al CRIC-GT, con el objetivo de minimizar el impacto de los mismos y mejorar la resiliencia digital.

Los CRIC podrán ser públicos, privados o público-privados, y formarán parte de un esquema nacional de coordinación con la Dirección y el CRIC-GT.

Lo relativo al registro, certificación, control, comunicación y verificación de los Equipos de Respuesta ante Incidentes de Ciberseguridad y Oficiales de la Seguridad de la Información será desarrollado por la vía reglamentaria.

Para un mejor entendimiento, se establece la siguiente clasificación:

a) **CRIC-Institucionales:** Las entidades del sector público deberán fortalecer sus capacidades en materia de ciberseguridad, de acuerdo a sus necesidades institucionales y a su presupuesto. Para el efecto, podrán crear un Equipo de Respuesta a Incidentes de Ciberseguridad, o como mínimo, contar con la contratación de un Oficial de Seguridad de la Información. Estos serán independientes de las dependencias de tecnologías de la información de las instituciones.

Los CRIC-Institucionales tendrán coordinación directa con el CRIC-GT.

b) **CRIC-Sectoriales:** El sector privado podrá agruparse por sectores estratégicos en CRIC-Sectoriales, con el objeto de brindar atención primaria coordinada a los incidentes cibernéticos o ciberataques de su sector, intercambiar información técnica y articular las acciones pertinentes con el CRIC-GT.

Los CRIC-Institucionales y CRIC-Sectoriales deberán reportar los incidentes cibernéticos o ciberataques al CRIC-GT, de conformidad con lo establecido en la presente Ley y su reglamento.

Artículo 30. Oficial de Seguridad de la Información. Las entidades públicas, privadas y público-privadas que creen un CRIC, deberán nombrar un Oficial de Seguridad de la Información, que será el enlace entre el CRIC-GT, CRIC-Sectorial y CRIC-Institucional.

El reglamento de la presente Ley desarrollará la descripción de sus funciones.

Artículo 31. Alertas y reportes sobre incidentes cibernéticos y ciberataques. Los CRIC-Sectoriales y CRIC-Institucionales tienen la obligación de alertar y reportar al CRIC-GT sobre los incidentes cibernéticos o ciberataques significativos de los que tenga conocimiento, resguardando la confidencialidad de las instituciones públicas, privadas o público-privadas, de la siguiente manera:

a) Cuando un incidente cibernético o ciberataque afecte una infraestructura crítica, la alerta deberá emitirse en un período no mayor de tres (3) horas, a partir de su detección;
b) Para otros casos, la alerta deberá emitirse en un período no mayor de seis (6) horas; y,
c) En un período no mayor de setenta y dos (72) horas, deberá remitirse el reporte completo sobre el incidente cibernético o ciberataque.

El CRIC-GT deberá implementar mecanismos de anonimización en los reportes de incidentes cibernéticos y ciberataques, para garantizar la confidencialidad, integridad y disponibilidad de la información, datos personales e institucionales, en lo público y privado.

Artículo 32. Coordinación con el régimen de prevención del lavado de dinero. La Dirección y el CRIC-GT coordinarán con la Superintendencia de Bancos, con la Comisión de Ciberseguridad del Sistema Bancario Nacional y, en lo relativo a inteligencia financiera, con la Intendencia de Verificación Especial, el intercambio de tipologías y alertas sobre incidentes cibernéticos vinculados al fraude y al lavado de dinero, conforme al Decreto Número 15-2026 del Congreso de la República, Ley Integral Para la Prevención y Represión del Lavado de Dinero u Otros Activos y del Financiamiento del Terrorismo. El Consejo Nacional de Ciberseguridad y el Consejo Nacional de Coordinación de los Esfuerzos contra el Lavado de Dinero u Otros Activos, el Financiamiento del Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción Masiva establecerán un mecanismo permanente de coordinación.

Los reportes de incidentes no contendrán información relativa a reportes de transacciones sospechosas ni revelarán su existencia. La exención de responsabilidad prevista en el artículo 31 de esta Ley se aplicará sin perjuicio de la que el artículo 37 del Decreto Número 15-2026 del Congreso de la República establece para los reportes a la Intendencia de Verificación Especial. La transmisión de información financiera protegida a autoridades extranjeras se regirá por el artículo 71 de esta Ley.

El oficial de seguridad de la información y el oficial de cumplimiento de una misma entidad coordinarán sus funciones conforme a la normativa de la Junta Monetaria y de la Superintendencia de Bancos, sin que esta Ley exija la creación de cargos adicionales.

Artículo 33. Niveles de respuesta ante incidentes cibernéticos. La gestión de los incidentes se realizará bajo los principios de competencia primaria, subsidiariedad y escalamiento, procurando que cada incidente sea atendido inicialmente en el nivel institucional más próximo y sea escalado cuando su naturaleza, impacto o complejidad exceda las capacidades o competencias de dicho nivel.

Para efecto de lo anterior, las competencias operativas de las entidades de la materia, se deberá atender un esquema escalonado de gestión de incidentes que permita ordenar la toma de decisiones, de la siguiente manera:

a) **Nivel 1. Incidente Institucional:** En casos de afectación localizada sin impacto crítico, la respuesta primaria estará a cargo de CRIC-Institucional.
b) **Nivel 2. Incidente Crítico Institucional**: En casos de afectación localizada con impacto crítico sobre una o varias instituciones, la respuesta deberá ser coordinada entre CRIC-Institucional y CRIC-GT.
c) **Nivel 3. Incidente Crítico Nacional:** En casos de afectación multisectorial con impacto crítico sobre la continuidad operativa nacional, la mitigación de incidentes cibernéticos estará bajo la responsabilidad coordinada del Consejo, DICIBER y CRIC-GT, actuando la unidad especializada del Ministerio de la Defensa Nacional en funciones subsidiarias y de apoyo especializado.
d) **Nivel 4. Incidente que afecte la Soberanía Nacional:** En casos de ataques que afecten la soberanía nacional, la respuesta inmediata estará a cargo de la unidad especializada del Ministerio de la Defensa Nacional, quien por mandato constitucional asumirá el liderazgo de las acciones, debiendo apoyarse en DICIBER y CRIC-GT para gestionar. Una vez que el ataque haya sido contenido y mitigado por dicha Unidad, regresará a ejercer funciones subsidiarias y de apoyo especializado a la ciberseguridad.

Cuando un incidente alcance los niveles 3 o 4, el Consejo se constituirá en Comité de Crisis para atender la emergencia.

Los niveles de actuación a que se refiere este artículo serán desarrollados por la Dirección y el Ministerio de la Defensa Nacional, según corresponda, y aprobados por el Consejo, en su protocolo de actuación correspondiente.

CAPÍTULO VI
ACCIONES DE CIBERDEFENSA

Artículo 34. Acciones de ciberdefensa. Para preservar la independencia, la soberanía, el honor de Guatemala, la integridad del territorio, la paz y la seguridad, en el

ciberespacio, el Ministerio de la Defensa Nacional, por conducto de su unidad especializada, desarrollará permanentemente las siguientes funciones:

a) Mantener comunicación y coordinación permanente con el Ministerio de Gobernación, a través de la Dirección Nacional de Ciberseguridad;
b) Colaborar y cooperar en aquellos casos en que un incidente cibernético o ciberamenaza afecte las infraestructuras críticas y comprometa la defensa nacional;
c) Dar apoyo especializado a la Dirección y al CRIC-GT en aquellos casos en que sus capacidades técnicas u operativas sean sobrepasadas;
d) Para efecto de dar cumplimiento a lo establecido en la anterior literal, deberá desarrollar en conjunto con la Dirección y el CRIC-GT un protocolo de actuación;
e) Dar protección preventiva y activa de redes militares y sistemas informáticos y tecnologías de la información y la comunicación que integren las infraestructuras críticas cuya afectación comprometa la defensa nacional;
f) Elaborar y actualizar el Catálogo de Infraestructuras Críticas Digitales;
g) Desarrollar el Protocolo de Acciones Defensivas y Ofensivas para la Protección de las Infraestructuras Críticas que atenten contra la Defensa Nacional, el cual deberá ser aprobado por el Consejo Nacional de Ciberseguridad;
h) Planificar, identificar, recolectar, procesar, analizar, producir, distribuir y difundir información relacionada con amenazas, riesgos y vulnerabilidades que correspondan a los ámbitos de la ciberdefensa y la defensa nacional, estableciendo los protocolos necesarios;
i) Dar apoyo a las operaciones militares de tierra, aire y mar;
j) Ser el punto de contacto a nivel internacional en materia de ciberdefensa, para brindar seguimiento, apoyo y recomendaciones, cuando le sea requerido;
k) Crear los marcos normativos y la doctrina para la ciberdefensa;
l) Establecer y actualizar las políticas, estrategias, planes y protocolos de ciberdefensa para la prevención, detección, contención, protección, recuperación de los sistemas y respuesta del Ministerio de la Defensa Nacional;
m) Diseñar y realizar programas de formación continua, entrenamiento especializado, simulacros técnicos y ejercicios conjuntos en materia de ciberdefensa, a nivel nacional e internacional;
n) Informar al Consejo Nacional de Ciberseguridad, mensualmente o cuando le sea requerido, sobre la atención, seguimiento y resolución de los incidentes gestionados para la ciberdefensa; y,
o) Asesorar técnicamente en el diseño de políticas, estrategias, programas y acciones en materia de ciberdefensa.

En el cumplimiento de las anteriores funciones, no se podrán vulnerar las garantías individuales y sociales preceptuadas en la Constitución Política de la República de Guatemala.

TÍTULO III
RÉGIMEN ADMINISTRATIVO SANCIONATORIO

CAPÍTULO ÚNICO
RÉGIMEN ADMINISTRATIVO SANCIONATORIO

Artículo 35. Sujetos obligados. Estarán sujetos al régimen administrativo sancionatorio de esta Ley los operadores de servicios esenciales y las personas individuales o jurídicas que administren, gestionen u operen sistemas informáticos cuya afectación pueda comprometer la continuidad de servicios esenciales, infraestructuras críticas, la seguridad de la información o el funcionamiento de sistemas estratégicos para el país.

El ente a cargo de la aplicación del régimen administrativo sancionatorio será la Dirección.

Artículo 36. Leyes especiales. No serán sujetos obligados las personas jurídicas de derecho público y privado sujetas a normativa específica, cuando esta ya regule lo relativo en materia de ciberseguridad.

Tampoco serán sujetos obligados las personas jurídicas reguladas por leyes de rango constitucional, las cuales se regirán exclusivamente por lo dispuesto en las mismas.

Artículo 37. Obligaciones para el manejo de datos y sistemas informáticos. Serán obligaciones de los sujetos obligados respecto al manejo de datos y sistemas informáticos las siguientes:

- **a)** Implementar medidas técnicas y organizativas para la protección de datos y sistemas informáticos apropiadas para garantizar un nivel mínimo de seguridad adecuado al riesgo;
- **b)** Actuar con el debido cuidado en calidad de garante durante el tratamiento de los datos y sistemas informáticos, para prevenir, detectar y mitigar los efectos de una posible amenaza o vulneración a los mismos;
- **c)** Cumplir con estándares internacionales, buenas prácticas o certificaciones reconocidas en materia de protección de datos y sistemas informáticos; y,
- **d)** Otras que sean establecidas en la presente Ley y su reglamento.

En cuanto a la debida gestión del riesgo cibernético, la Dirección emitirá los lineamientos técnicos correspondientes por la vía reglamentaria.

Artículo 38. Clasificación de las infracciones. Las infracciones administrativas en materia de ciberseguridad se clasifican en leves, graves y gravísimas, de conformidad con lo establecido en la presente Ley.

El reglamento de la presente Ley desarrollará las conductas constitutivas de infracciones y las respectivas sanciones, de conformidad con los estándares y las buenas prácticas internacionales.

Artículo 39. Procedimiento administrativo sancionatorio. Cuando la autoridad competente detecte o reciba denuncia sobre alguna presunta infracción, iniciará la formación del expediente respectivo, aplicando el siguiente procedimiento administrativo:

a) Formulación de cargos al presunto infractor;
b) Notificación y concesión de audiencia por un plazo de 2 días;
c) En el plazo de la audiencia, el presunto infractor se pronunciará sobre los cargos formulados en su contra, aceptándolos o negándolos, y propondrá sus pruebas de descargo;
d) Cuando el infractor aceptare los cargos formulados, podrá subsanarlos a satisfacción de la autoridad, de conformidad con esta Ley y su reglamento;
e) Se abrirá a prueba por el plazo de 5 días; y,
f) La autoridad administrativa competente dictará la resolución que confirme o no los cargos y, en su caso impondrá las medidas correctivas y/o sanciones respectivas.

En el caso de las medidas correctivas, la autoridad competente concederá un plazo prudencial al infractor para que ejecute las mismas.

La aplicación de las sanciones administrativas se hará sin perjuicio de las sanciones aplicables por la comisión de posibles delitos, por lo que el órgano competente deberá realizar la denuncia penal respectiva cuando existan indicios razonables sobre la posible comisión de un delito.

Artículo 40. Impugnaciones. Contra lo resuelto por la autoridad competente, procederán los recursos administrativos previstos en el Decreto Número 119-96 del Congreso de la República, Ley de lo Contencioso Administrativo.

Artículo 41. Subsanación y medidas correctivas. Velando por la protección de los sistemas informáticos y los datos que estos contienen, la autoridad competente deberá privilegiar la subsanación y la imposición de medidas correctivas sobre las sanciones administrativas previstas, cuando aquellas resulten suficientes para garantizar el cumplimiento de la misma.

Artículo 42. Destino de las multas. El monto recaudado por concepto de las multas administrativas impuestas en aplicación del régimen administrativo sancionatorio, formará parte de los fondos privativos de la Dirección y deberá destinarse para promover acciones y programas de prevención, formación e investigación en materia de ciberseguridad.

Artículo 43. Exclusión de responsabilidad administrativa. No se apreciarán como infracciones administrativas, las acciones que sean realizadas bajo la práctica autorizada en la que expertos en ciberseguridad simulan incidentes o ataques cibernéticos, como una actividad legítima de prevención, formación, investigación y evaluación que permita encontrar y corregir fallos de seguridad en redes o sistemas, con el objeto de anticiparse a la brecha de datos, robo de información o daños a los datos o infraestructuras críticas.

Asimismo, las acciones realizadas por docentes o estudiantes, cuando exista finalidad académica legítima de formación, investigación, evaluación o divulgación responsable, sin

ánimo de lucro, sin haber causado daño y en actuación bajo protocolos reconocidos de comunicación de vulnerabilidades.

La legalidad, objeto y alcance de las acciones contempladas en este artículo deberán ser previamente definidas entre las partes en un contrato o convenio, según corresponda.

TÍTULO IV
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 44. Acceso ilícito. Comete el delito de acceso ilícito, quien acceda sin autorización o excediendo la autorización que posea, por cualquier método, a todo o parte de un sistema informático o sistema que utilice tecnologías de la información y la comunicación, cuando dicho acceso se realice infringiendo medidas de seguridad. Al responsable de este delito se le impondrá una pena de prisión de 4 años a 6 años.

Artículo 45. Interceptación ilícita. Comete el delito de interceptación ilícita quien, sin autorización y por cualquier medio o forma, intercepte datos informáticos en transmisiones no públicas 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 5 a 8 años.

Artículo 46. 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 de este delito se le impondrá una pena de prisión de 5 a 7 años.

Artículo 47. Ataque a la integridad del sistema informático. Comete el delito de ataque a la integridad del sistema informático quien, sin autorización, obstaculice de propósito el funcionamiento normal de un sistema informático o sistemas que utilicen tecnologías de la información y la comunicación, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos. Al responsable de este delito se le impondrá una pena de prisión de 5 a 8 años.

CAPÍTULO II
DELITOS INFORMÁTICOS

Artículo 48. Falsificación informática. Comete el delito de falsificación informática quien, sin autorización, introduzca, altere, borre o suprima datos o registros informáticos, y con ello genere datos no auténticos para que sean tomados o utilizados a efectos legales 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 2 a 6 años.

Artículo 49. Apropiación de identidad ajena. Comete el delito de apropiación de identidad ajena quien, sin autorización, utilizando cualquier forma o medio, 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 2 a 4 años. Cuando el hecho se realice infringiendo medidas de seguridad, se impondrá una pena de prisión de 3 a 6 años.

Artículo 50. 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, produzca un daño, perjuicio o defraudación en el patrimonio de otra persona, individual o jurídica, mediante:

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

Al responsable de este delito se le impondrá una pena de prisión de 4 a 8 años.

Artículo 51. Abuso de dispositivos. Comete el delito de abuso de dispositivos quien, sin autorización y con la finalidad de cometer o facilitar la comisión de cualquiera de los delitos previstos en los artículos 44 al 50 de la presente Ley, realice cualquiera de los actos siguientes:

a) Produzca, venda, obtenga para su utilización, posea, importe, difunda o de cualquier otra forma ponga a disposición:

1. 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 44 al 50 de la presente Ley; o,

2. Cualquier contraseña, código 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 44 al 50 de la presente Ley; o,

b) Cree, utilice, altere, capture, grabe, copie o transfiera de un dispositivo a otro o a 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, simultánea o independiente de dichos servicios o sistemas legítimamente obtenidos por un tercero; o bien, con el fin de ser utilizados para cometer cualquiera de los delitos previstos en los artículos del 44 al 50 de la presente Ley.

Al responsable de este delito se le impondrá una pena de prisión de 3 a 6 años.

No se interpretará que el presente artículo impone responsabilidad penal cuando las conductas descritas en este artículo no tengan por objeto la comisión de alguno de los delitos previstos en los artículos 44 al 50 de la presente Ley, como en el caso de las pruebas autorizadas o de la protección de un sistema informático o sistema que utilice las tecnologías de la información y la comunicación.

Artículo 52. 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 Número 17-73 del Congreso de la República de Guatemala, Código Penal; se cometan con fines de comercialización 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 53. Agravantes generales. Las penas correspondientes a los delitos previstos en los artículos 44 al 51 de la presente Ley, cuando sea aplicable, se aumentarán en una tercera parte en cualquiera de los casos siguientes:

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. Si el hecho hubiera sido realizado por servidor o funcionario público en contra de la institución para la que labora o laboraba, además de la pena aplicable, será inhabilitado para ejercer funciones públicas por un período de 7 años;

b) Cuando de la acción realizada resulte la denegación de acceso, supresión o modificación de datos confidenciales, reservados o de seguridad nacional, contenidos en un sistema informático o sistema que utilice tecnologías de la información y la comunicación;

c) Cuando el acto se realice para recibir ilícitamente beneficio pecuniario o de cualquier otra índole, ya sea propio o para terceros, o para gozar de los servicios ofrecidos a través de cualquiera de estos sistemas. Esta circunstancia no será aplicable al delito previsto en el artículo 50 cuando esto ya constituya elemento del tipo penal.

Las penas se aumentarán en dos terceras partes, cuando el hecho se cometa en contra de las infraestructuras críticas digitales, de conformidad con lo que establece la ley.

CAPÍTULO III
RESPONSABILIDAD Y PENAS ACCESORIAS

Artículo 54. Responsabilidad civil o administrativa de las personas individuales. Las sanciones penales establecidas en la presente Ley para personas individuales se aplicarán sin perjuicio de las responsabilidades civiles o administrativas que correspondan.

Artículo 55. Responsabilidad y penas accesorias de personas jurídicas. En lo relativo a las personas jurídicas, independientemente de la responsabilidad penal de sus 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 cien mil quetzales (Q100,000.00) a trescientos mil quetzales (Q300,000.00) y, atendiendo a la gravedad y circunstancias en que se cometió el delito, se le impondrá una o varias de las penas siguientes:

a) Inmovilización de cuentas bancarias y bienes inmuebles, siempre y cuando se garanticen las prestaciones laborales, según lo determine el órgano jurisdiccional competente, hasta por el monto que hubieren obtenido como efecto del delito.
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) Inhabilitación para participar con el Estado en los procesos de concurso, celebrar contratos y ser proveedores de este, de forma definitiva o por un período no menor de cinco años, cuando el agraviado del delito sea el Estado.
d) Inhabilitación para participar en actividades destinadas a la captación de títulos valores, de forma definitiva o por un período no menor de cinco años.
e) Comiso de los bienes o ganancias que se hayan obtenido por la comisión del delito.
f) Publicación de la sentencia pronunciada o la difusión de esta, de conformidad con el procedimiento establecido en el Decreto Número 17-73 del Congreso de la República, Código Penal.

En caso de reincidencia, se ordenará la cancelación definitiva de la personalidad jurídica, sin perjuicio de la aplicación de las sanciones antes señaladas.

La presente disposición no se aplicará cuando la persona jurídica sea sujeto pasivo de la acción delictiva. En este caso, deberá ser valorado el nivel de cumplimiento del deber de diligencia en la implementación de medidas razonables de seguridad digital atendiendo a la naturaleza de la entidad.

Las disposiciones contenidas en este artículo no serán aplicables a las personas jurídicas de derecho público y privado sujetas a normativa específica, cuando esta ya regule lo relativo en materia de ciberseguridad.

Tampoco serán aplicables las disposiciones contenidas en este artículo a las personas jurídicas reguladas por leyes de rango constitucional, las cuales se regirán exclusivamente por lo dispuesto en las mismas.

Para imponer las sanciones previstas en este artículo, las autoridades competentes deberán garantizar el respeto al derecho de defensa, la proporcionalidad de la medida y el debido proceso.

Artículo 56. Exclusión de responsabilidad penal. No se apreciarán como delitos, las acciones que sean realizadas bajo la práctica autorizada en la que expertos en ciberseguridad simulan incidentes o ataques cibernéticos, como una actividad legítima de prevención, formación, investigación y evaluación que permita encontrar y corregir fallos de seguridad en redes o sistemas, con el objeto de anticiparse a la brecha de datos, robo de información o daños a los datos o infraestructuras críticas.

Asimismo, las acciones realizadas por docentes o estudiantes, cuando exista finalidad académica legítima de formación, investigación, evaluación o divulgación responsable, sin ánimo de lucro, sin haber causado daño y en actuación bajo protocolos reconocidos de comunicación de vulnerabilidades.

La legalidad, objeto y alcance de las acciones contempladas en este artículo deberán ser previamente definidas entre las partes en un contrato o convenio, según corresponda.

TÍTULO V
DISPOSICIONES PROCEDIMENTALES

CAPÍTULO I
DISPOSICIONES PROCEDIMENTALES

Artículo 57. Acción pública. Los delitos regulados en la presente Ley son de acción pública.

Artículo 58. Ámbito de aplicación de las disposiciones procedimentales. Las normas del presente capítulo se aplicarán a:

- **a)** Los delitos previstos en la presente Ley.
- **b)** La obtención de indicios, medios de investigación o pruebas informáticas, digitales o electrónicas, de los delitos contenidos en la presente Ley.
- **c)** La rebaja de penas o beneficios penales de conformidad con la presente Ley.

La rebaja de penas o beneficios penales a las personas sentenciadas no serán ejecutadas, en tanto estas no hayan efectuado la reparación digna e integral a las víctimas o agraviados, en sus componentes de indemnización, restitución, rehabilitación, satisfacción y garantía de no repetición, según corresponda. Tampoco podrán hacerse efectivas, en tanto no hayan devuelto o entregado a las víctimas el incremento patrimonial fruto del delito.

Artículo 59. 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 Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal.

Artículo 60. Valoración de la prueba. Los órganos jurisdiccionales deberán valorar los medios probatorios incorporados al proceso, siendo determinante que hayan sido obtenidos mediante el procedimiento establecido en el Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal.

Artículo 61. Diligencias de urgencia para el aseguramiento de datos. Cuando exista peligro de que los datos objeto de una investigación puedan ser alterados o suprimidos durante la etapa preparatoria, se solicitarán las diligencias de urgencia para el aseguramiento de los mismos, de conformidad con lo establecido en el Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal.

Artículo 62. Orden de acceso y envío de datos. En caso de necesidad o razonabilidad comprobada, el órgano jurisdiccional competente podrá ordenar a los proveedores de servicios de tecnologías de la información y la comunicación, las siguientes medidas:

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 esté bajo su poder o control y que se vinculen con la investigación de un delito.
b) Que 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, período de servicios y lugar de ubicación de los equipos.

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

Artículo 63. 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 correspondientes.

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

La orden de registro delimitará su objeto, los sistemas comprendidos, la información buscada, los medios de ejecución, los responsables y el tiempo de la diligencia, y privilegiará la extracción selectiva y la copia forense sobre la ocupación o interrupción de sistemas productivos. La posibilidad de acceder lícitamente desde un sistema a otro conectado no autorizará un registro general de las redes conectadas: la extensión del registro a otros sistemas, cuentas o dispositivos requerirá nueva autorización judicial que los individualice y fundamente su necesidad. En servicios compartidos o en la nube, la delimitación protegerá los datos de los demás clientes del proveedor. Se adoptarán medidas para excluir datos manifiestamente ajenos a la investigación, salvaguardar comunicaciones privilegiadas y mantener registro verificable de las actuaciones y cadena de custodia.

Artículo 64. Aseguramiento digital como medida cautelar penal. En el marco de una investigación por delitos informáticos o relacionados con un evento que afecte la ciberseguridad de un sistema informático, mediante autorización judicial, se deberá ordenar el aseguramiento digital de redes, bases de datos o activos digitales sin necesidad del secuestro de los equipos, debiendo cumplir las siguientes condiciones:

a) Que exista indicio razonable que contenga información vinculada a la investigación penal;
b) Se garantice la integridad, trazabilidad y cadena de custodia de la información; y,
c) Se respete el derecho de defensa, garantizando la continuidad de las operaciones y se permita el control judicial de la medida.

El aseguramiento digital podrá consistir en restricción lógica, acceso remoto controlado, copia forense o cualquier otra técnica que preserve la evidencia sin alterar su contenido ni vulnerar derechos fundamentales.

La medida prevista en el presente artículo únicamente podrá decretarse en investigaciones relacionadas con delitos informáticos regulados en la presente Ley, y no podrá aplicarse por analogía o extensión a otro tipo de delitos, en observancia del principio de legalidad.

Artículo 65. Medidas cautelares para el aseguramiento y tratamiento 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 y el plazo de duración. Dicho plazo no podrá exceder de dos meses, prorrogables 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 de Guatemala, en particular la inviolabilidad de las comunicaciones privadas y la protección de los datos personales, siendo nula de pleno derecho cualquier autorización que se aparte de los límites aquí previstos.

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

Antes de ordenar una medida que pueda interrumpir servicios financieros críticos o sistemas de pagos, el órgano jurisdiccional solicitará por canal reservado informe técnico del Banco de Guatemala o de la Superintendencia de Bancos, según su competencia, sobre las alternativas y los efectos de la ejecución. El informe se emitirá dentro del plazo que fije el juez según la urgencia, sin comunicar información innecesaria de la investigación y sin que otorgue derecho de veto a la autoridad consultada. Si la demora creara un riesgo grave e inminente para la evidencia o el servicio, el juez podrá resolver de inmediato, motivando esa circunstancia y disponiendo la coordinación técnica simultánea o inmediatamente posterior.

Se preferirán la copia forense, el acceso de lectura, la segmentación o el bloqueo específico cuando sean suficientes. La orden distinguirá los sistemas y datos de terceros ajenos al proceso y establecerá la cadena de custodia, el registro de accesos y la restauración segura. La interrupción de transmisiones se revisará judicialmente al menos cada veinticuatro horas mientras afecte un servicio esencial y cesará cuando deje de ser necesaria; el plazo máximo previsto en este artículo no autoriza mantener desconectado el servicio durante todo ese período y la prórroga única que el artículo admite requerirá motivación individualizada.

Artículo 66. Comiso. El órgano jurisdiccional competente podrá ordenar el comiso de los objetos o instrumentos del delito, debiendo observarse lo regulado en el Decreto Número 17-73 del Congreso de la República de Guatemala, Código Penal; Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal; Decreto Número 21-2006 del Congreso de la República de Guatemala, Ley Contra la Delincuencia Organizada; y Decreto Número 15-2026 del Congreso de la República de Guatemala, Ley Integral para la Prevención y Represión del Lavado de Dinero u Otros Activos y del Financiamiento del Terrorismo.

CAPÍTULO II
COOPERACIÓN PROCESAL INTERNACIONAL

Artículo 67. 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 los tratados y convenios internacionales de los que Guatemala sea parte.

Artículo 68. Requerimiento internacional de información. En caso de requerimiento internacional de información, dentro del marco de una investigación de carácter penal relacionada a los delitos tipificados en la presente Ley, en cuanto a las solicitudes de aseguramiento de datos, 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 los tratados y convenios internacionales 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, sí se ordenará su revelación para fines de la investigación, debiendo ser justificado por el Ministerio Público ante el órgano jurisdiccional competente, quien emitirá la resolución que en derecho corresponda.

Artículo 69. Preservación rápida de datos transfronterizos. Las autoridades competentes de cada país podrán ordenar la preservación inmediata de datos informáticos relevantes para una investigación penal, aún cuando se encuentren almacenados en sistemas ubicados fuera del territorio nacional, conforme a tratados internacionales y bajo control judicial. La preservación no implicará acceso ni revelación de los datos hasta que exista autorización judicial expresa.

Artículo 70. Admisibilidad de pruebas digitales obtenidas en el extranjero. Las pruebas digitales obtenidas mediante cooperación internacional serán reconocidas y valoradas en los tribunales nacionales, siempre que se hayan obtenido conforme a tratados internacionales vigentes y bajo respeto de garantías procesales fundamentales, incluyendo el debido proceso, la proporcionalidad y el control judicial.

Artículo 71. Asistencia mutua urgente. En casos de delitos informáticos que requieran medidas inmediatas, las autoridades nacionales podrán brindar o solicitar asistencia mutua urgente para la obtención de datos de tráfico, interceptación de comunicaciones o acceso a información crítica, aún en ausencia de tratado bilateral, siempre que exista solicitud formal y control judicial.

La información financiera protegida por el artículo 63 del Decreto Número 19-2002 y por el Decreto Número 15-2026, ambos del Congreso de la República, solo se transmitirá a autoridades extranjeras por conducto del Ministerio Público con orden judicial o por los canales previstos en dichas leyes y en los tratados vigentes.

Artículo 72. Compatibilidad con derecho internacional aplicable. Las solicitudes de cooperación internacional en materia de ciberseguridad deberán tramitarse conforme a procedimientos compatibles con el derecho penal internacional, evitando en lo posible rechazos o demoras. El Ministerio Público será responsable de justificar la solicitud y garantizar la protección de derechos fundamentales.

Artículo 73. Asistencia jurídica internacional en materia de ciberdelincuencia. El Estado prestará y solicitará asistencia jurídica internacional en la investigación, persecución y sanción de los delitos previstos en la presente Ley, de conformidad con la legislación penal vigente, los tratados internacionales ratificados por Guatemala, los principios de reciprocidad y cooperación internacional, y en ausencia de tratado bilateral, mediante solicitud formal y bajo control judicial. Esta asistencia podrá comprender, entre otras, las siguientes medidas, previa autorización judicial, cuando corresponda:

a) La preservación rápida y obtención expedita de datos informáticos, incluso cuando se encuentren almacenados en sistemas ubicados fuera del territorio nacional.

b) El acceso, aseguramiento y remisión de evidencia digital.

c) La identificación de usuarios, suscriptores y dispositivos.

d) La ejecución de actos de investigación y medidas cautelares.

e) La admisibilidad y reconocimiento en tribunales nacionales de pruebas digitales obtenidas en el extranjero, siempre que se hayan recabado conforme a tratados internacionales vigentes y bajo respeto de garantías procesales fundamentales.

f) Cualquier otra diligencia necesaria para el esclarecimiento de los hechos.

Las solicitudes se tramitarán con carácter prioritario y mediante los canales más expeditos disponibles, garantizando en todo momento el debido proceso, el control judicial y el respeto a los derechos y garantías constitucionales.

TÍTULO VI
FORTALECIMIENTO INSTITUCIONAL

CAPÍTULO ÚNICO
FORTALECIMIENTO INSTITUCIONAL

Artículo 74. Fortalecimiento del Ministerio Público 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; así mismo, deberá fortalecer la Unidad de Atención Permanente en materia de la presente Ley.

El Ministerio Público deberá contratar y capacitar a personal especializado en ciberseguridad y ciberdelitos para garantizar el debido cumplimiento de lo dispuesto en la presente Ley, así como, generar cualquier otra capacidad que sea necesaria en la materia.

Artículo 75. Red de Asistencia Mutua Contra Delitos Informáticos (RED 24/7 Guatemala). El Ministerio Público creará una unidad de atención permanente, como punto de contacto localizable las veinticuatro horas del día y siete días a la semana, integrándose a través de redes a las que Guatemala se adhiera o forme parte, la que se denominará Red de Asistencia Mutua Contra Delitos Informáticos o RED 24/7 Guatemala, con el objeto de garantizar la prestación de asistencia 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 digitales en la comisión de un hecho delictivo.

El Ministerio Público deberá contratar y capacitar a personal especializado en ciberseguridad y ciberdelitos para garantizar su disponibilidad y una respuesta técnica y eficiente ante las solicitudes internacionales de cooperación que deba de atender la RED 24/7 Guatemala.

La asistencia que brindará la RED 24/7 Guatemala incluirá todos los actos que tiendan a facilitar las medidas de conformidad con la legislación nacional y lo establecido en la presente Ley, para la conservación de datos, obtención de indicios o pruebas, suministro de información y otros.

Artículo 76. 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 77. Creación de los órganos jurisdiccionales especializados. El Organismo Judicial deberá garantizar la aplicación de la presente Ley a través de la creación e implementación de órganos jurisdiccionales especializados.

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 78. Fortalecimiento de la Policía Nacional Civil. Para el cumplimiento de las disposiciones contenidas en la presente Ley, el Ministerio de Gobernación deberá poner a disposición de la Policía Nacional Civil todo lo necesario para garantizar el fortalecimiento de la Dirección de Ciberseguridad y Ciberdelincuencia, con los recursos presupuestarios, físicos, materiales, científicos y humanos que le permitan el cumplimiento del objeto y demás disposiciones de esta Ley.

Artículo 79. Fortalecimiento del Instituto de la Defensa Pública Penal. Para el cumplimiento de las disposiciones contenidas en la presente Ley, el Instituto 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 80. Fortalecimiento del Ministerio de la Defensa Nacional. Para el cumplimiento de las funciones de ciberdefensa que dispone la presente Ley, el Ministerio de la Defensa Nacional deberá crear una unidad especializada en la materia y dotarla de los recursos humanos, presupuestarios, físicos, materiales y científicos necesarios que le permitan el adecuado cumplimiento del objeto y demás disposiciones de la presente Ley.

Artículo 81. Ministerio de Educación. El Ministerio de Educación, en coordinación con la Dirección, deberán definir los contenidos relacionados a la materia de la presente Ley, con enfoque teórico y práctico, adaptados a cada nivel escolar, para incluir en el Currículo Nacional Base o el pénsum de estudios vigente.

Para el efecto, podrán promover acciones y coordinar alianzas y convenios con otras instituciones u organizaciones de carácter público, privado o público-privado, para realizar actividades de fomento y educativas, con el objeto de formar una ciudadanía consciente, educada y responsable acerca del alto valor que tiene la ciberseguridad y demás materias relacionadas para el desarrollo y la protección de los derechos en el entorno digital.

Artículo 82. 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, buscará 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 la legislación vigente.

Artículo 83. Política Nacional de Ciberseguridad. La Política Nacional de Ciberseguridad deberá incorporar lineamientos específicos a corto, mediano y largo plazo a cerca del abordaje integral de la materia de ciberseguridad en el país, de conformidad con el objeto y demás disposiciones de la presente Ley. La misma será elaborada por la Dirección y aprobada por el presidente de la República.

TÍTULO VII
DISPOSICIONES TRANSITORIAS, DEROGATORIAS Y FINALES

CAPÍTULO ÚNICO
DISPOSICIONES TRANSITORIAS, DEROGATORIAS Y FINALES

Artículo 84. Plazo de implementación del CRIC-GT. El Centro de Respuesta a Incidentes de Ciberseguridad de Guatemala (CRIC-GT) deberá encontrarse en funcionamiento en un plazo máximo de dieciocho (18) meses a partir de la entrada en vigencia de la presente Ley.

Artículo 85. Presupuesto. El Ministerio de Finanzas Públicas deberá asignar una partida presupuestaria específica, con fuente de financiamiento de los ingresos tributarios sin destino específico u otras fuentes que se especifiquen en el Presupuesto General de Ingresos y Egresos del Estado vigente, para la implementación y funcionamiento de las instituciones creadas por la presente Ley.

Las demás instituciones mencionadas en la presente Ley, al momento de entrar en vigencia la misma, de ser necesario, reprogramarán su presupuesto del ejercicio fiscal vigente para dar cumplimiento a las obligaciones que esta establece y programarán anualmente los recursos necesarios para su cumplimiento.

Las dependencias del Organismo Ejecutivo, entidades descentralizadas y autónomas, desde el marco de su competencia y conforme a las necesidades y vulnerabilidades identificadas por el Consejo Nacional de Ciberseguridad, deberán incluir en su proceso de planificación, el presupuesto necesario para la materia de ciberseguridad.

Artículo 86. Criterios para las contrataciones del Estado en ciberseguridad y ciberdefensa. Las instituciones del sector público podrán adquirir bienes, equipos, servicios, sistemas o tecnologías de la información y comunicación destinados al fortalecimiento y protección en materia de ciberseguridad y ciberdefensa, conforme a lo establecido en la Ley de Contrataciones del Estado y su reglamento.

Para determinar cuál es la oferta más conveniente y favorable para los intereses del Estado, deberán aplicarse los criterios siguientes: calidad, precio, características, cumplimiento de certificaciones y seguridad, debiendo ser criterios objetivos, técnicos, verificables y definidos previamente en las respectivas bases, términos de referencia o instrumento similar.

Artículo 87. Se adiciona la literal r) al artículo 36 del Decreto Número 114-97 del Congreso de la República de Guatemala, Ley del Organismo Ejecutivo, el cual queda así:

"r) Ejercer las funciones específicas en materia de ciberseguridad."

Artículo 88. Se adiciona la literal f) al artículo 37 del Decreto Número 114-97 del Congreso de la República de Guatemala, Ley del Organismo Ejecutivo, el cual queda así:

"f) Ejercer las funciones específicas en materia de ciberdefensa."

Artículo 89. Se reforma el párrafo primero del artículo 22 del Decreto Número 18-2008 del Congreso de la República de Guatemala, Ley Marco del Sistema Nacional de Seguridad, el cual queda así:

"Artículo 22. Ámbito de Gestión de Riesgos y Defensa Civil. Constituye la capacidad del Estado para desarrollar e implementar políticas de prevención, preparación, mitigación, respuesta y recuperación ante eventos de orden natural y social que puedan afectar a la población, sus bienes y entorno, a nivel nacional, departamental y municipal. Actúa bajo la responsabilidad del presidente de la República por conducto de la Coordinadora Nacional para la Reducción de Desastres -CONRED-."

Artículo 90. Coordinación interinstitucional. Para efecto de gestionar eventos de orden natural o social que sean competencia de la Coordinadora Nacional para la Reducción de Desastres -CONRED- y que estén vinculados a la ciberseguridad o la ciberdefensa, las autoridades competentes deberán establecer mecanismos de coordinación.

Artículo 91. Se adiciona la literal i) al artículo 2 del Decreto Número 21-2006 del Congreso de la República, Ley Contra la Delincuencia Organizada, el cual queda así:

"i) De los contenidos en la Ley Marco 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 Marco de Ciberseguridad y en demás cuerpos normativos relacionados con la materia."

Artículo 92. Derogatorias. Se derogan los artículos 274 "A", 274 "B", 274 "E", 274 "F" y 274 "G" del Decreto Número 17-73 del Congreso de la República de Guatemala, Código Penal.

Artículo 93. Fortalecimiento del marco normativo para la protección del entorno digital. Para fortalecer la protección de los derechos en el entorno digital, la autoridad competente deberá impulsar la elaboración y aprobación de un marco normativo robusto y armonizado que brinde certeza jurídica a las demás materias relacionadas a la ciberseguridad de acuerdo con la evolución de las tecnologías.

Artículo 94. Reglamento de la ley. El Organismo Ejecutivo, por conducto del Ministerio de Gobernación, deberá aprobar el reglamento de la presente Ley dentro de seis (6) meses a partir de la entrada en vigencia de la presente Ley.

Artículo 95. Armonización reglamentaria. Dentro de seis (6) meses, a partir de la entrada en vigencia de la presente Ley, el Ministerio de Gobernación y el Ministerio de la Defensa Nacional deberán adecuar sus reglamentos orgánicos internos y demás normativa interna reglamentaria, conforme a lo establecido en la presente Ley.

Asimismo, dentro de doce (12) meses, a partir de la entrada en vigencia de la presente Ley, las demás entidades vinculadas a la ciberseguridad deberán adecuar sus instrumentos, manuales y/o protocolos necesarios para el cumplimiento de sus funciones de conformidad con lo establecido en esta Ley.

Artículo 96. Cuerpo de seguridad del Estado. Dentro del plazo de seis (6) meses, a partir de la entrada en vigencia de la presente Ley, el Organismo Ejecutivo deberá adecuar el artículo 9 del Acuerdo Gubernativo Número 18-98, Reglamento de la Ley de Servicio Civil, para incorporar a la Dirección y sus dependencias como cuerpo de seguridad del Estado.

Artículo 97. Vigencia. El presente Decreto fue declarado de urgencia nacional, aprobado en un único debate, con el voto favorable de las dos terceras partes del número total de diputados que integran el Congreso de la República, y entrará en vigencia treinta 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 TRES DE NOVIEMBRE DE DOS MIL VEINTISÉIS.

CONGRESO DE LA REPÚBLICA - GUATEMALA, C. A.

LUIS ALBERTO CONTRERAS COLÍNDRES
PRESIDENTE

JUAN CARLOS RIVERA ESTEVEZ
SECRETARIO

GERSON GEOVANNY BARRAGÁN MORALES
SECRETARIO

PALACIO NACIONAL: Guatemala, dieciséis de noviembre del año dos mil veintiséis.

PUBLÍQUESE Y CÚMPLASE

AREVALO DE LEON

Marco Antonio Villeda Sandoval
Ministro de Gobernación

Carlos Ramiro Martínez Alvarado
Ministro de Relaciones Exteriores

Henry David Saenz Ramos
Ministro de la Defensa Nacional

Norma Zea Osorio
Ministra de Comunicaciones
Infraestructura y Vivienda

Jonathan Kiril Thomas Menkos Zeissig
Ministro de Finanzas Públicas

Lic. Juan Gerardo Guerrero Garnica
SECRETARIO GENERAL
DE LA PRESIDENCIA DE LA REPÚBLICA

(E-769-2026)–17–noviembre