**ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA**

# PROYECTO DE LEY
# LEY DE CIBERSEGURIDAD DE COSTA RICA

**JOSE JOAQUIN HERNANDEZ ROJAS**
**Y OTROS SEÑORAS DIPUTADAS Y SEÑORES DIPUTADOS**

**EXPEDIENTE N° 23.292**

**PROYECTO DE LEY**

**“LEY DE CIBERSEGURIDAD DE COSTA RICA”**

**Expediente N° 23.292**

**ASAMBLEA LEGISLATIVA:**

A nivel mundial se reconoce que las tecnologías digitales (TD) y en especial las tecnologías de la información y la comunicación (TIC) son un catalizador para el desarrollo económico, social y cultural, dado que facilitan el acceso a incalculables recursos y que además de la comunicación, promueven la innovación, la eficiencia, la transparencia, y la prosperidad socioeconómica de los países.

Costa Rica, consciente de ello, ha apostado por una fuerte promoción del uso de las TIC para impulsar el desarrollo nacional y consolidar una sociedad de la información y el conocimiento preparada para enfrentar los desafíos de la cuarta revolución industrial y la transformación digital. De ello, son reflejo la Política Nacional de Sociedad y Economía Basada en el Conocimiento 2022-2050 (PNSEBC), el Plan Nacional de Ciencia, Tecnología e Innovación 2022-2027 (PNCTI) y la Estrategia de Transformación Digital (2017-2022), esto último, en proceso de actualización y consulta, entre otras.

Sin embargo, con los altos índices de conectividad y acceso a las TIC, la apuesta por la digitalización del Gobierno, el almacenamiento masivo de datos sensibles, y la acelerada transformación impulsada por la pandemia, surgen riesgos y vulnerabilidades propias del ciberespacio que exponen a todos los sectores de la sociedad a consecuencias perjudiciales.

El resultado de esta transición hacia lo digital es un extraordinario aumento de ataques cibernéticos, en el contexto de un ecosistema digital de vulnerabilidades ya

amplificadas que incluye más de 20.000 millones de dispositivos de internet de las cosas (IoT, por sus siglas en inglés) conectados en todo el mundo. Incluso antes de la pandemia, las brechas de ciberseguridad y las filtraciones de datos se estaban convirtiendo en los principales obstáculos de la economía digital. Los cibercriminales están aprovechando rápidamente los nuevos vectores de ataque y se benefician de los vacíos en la cooperación de las fuerzas del orden público en las diferentes jurisdicciones (Barmpaliou, 2021).

Según el *Informe de Riesgos Globales 2020* del Foro Económico Mundial, **el riesgo de ciberataques a la infraestructura crítica de los países y el fraude o robo de datos se clasificaron entre los diez principales riesgos con mayor probabilidad de ocurrir**, mientras que la reciente Perspectiva de Riesgos del COVID-19 del Foro Económico Mundial, identificó a los ciberataques como la tercera mayor preocupación. La infraestructura crítica refiere a aquellos sistemas de información que soportan la prestación de servicios esenciales para la sociedad.

Por otra parte, según el Reporte "*Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y El Caribe*" de 2021, elaborado en conjunto por el BID y la OEA, se estimó que **los daños por delitos cibernéticos alcanzarían los US$6000 millones para el 2021**, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo. Además del costo financiero, el cibercrimen y los ciberataques socavan la confianza de los usuarios en la economía digital.

Los cibercriminales que acceden a la red con fines ilícitos han aprovechado esta nueva realidad, y muestra de ello es el desarrollo de herramientas y medios cada vez más sofisticados para perpetrar sus ataques cibernéticos (como son, por ejemplo, los ataques de "ransomware-as-a-service". Esta intensificación modernización de la ciberdelincuencia, hace necesario sofisticar también las defensas de ciberseguridad de las organizaciones y gobiernos.

En el caso particular de la administración pública, la información masiva y sensible que ésta almacena sobre la población y sobre el quehacer gubernamental, así como los sistemas e infraestructura crítica que respalda los servicios esenciales que proveen los gobiernos, son un blanco especialmente atractivo para los cibercriminales.

En todo el mundo, incluida Costa Rica recientemente, son constantes los ataques contra infraestructuras críticas que hacen necesaria la suspensión o interrupción de los sistemas, lo que pone en riesgo la prestación de servicios esenciales para la población, como la salud y la seguridad nacional.

Los incidentes de ciberseguridad han tenido lugar durante años, pero la mayoría han permanecido fuera de la atención pública hasta la última década, los recientes incidentes de gran repercusión que han afectado a los ciudadanos han catapultado el tema al discurso nacional y a la atención legislativa y regulatoria. Estamos entrando en una nueva era de la ciberseguridad, en la que los gobiernos, los organismos reguladores y las empresas de todo el mundo deben trabajar unidos para aumentar la supervisión de los incidentes de ciberseguridad (McKinsey, 2022).

La ciberseguridad es, desde luego, un elemento habilitador e imprescindible para la transformación digital y la seguridad nacional, sí los activos digitales, los datos, y las infraestructuras que soportan los servicios esenciales para la población no están protegidos, no puede haber transformación digital ni se pueden aprovechar los beneficios que derivan de ese fenómeno.

En el caso concreto de Costa Rica, su estado de madurez en materia de ciberseguridad es apenas formativo. Así lo acreditan el BID y la OEA en su Reporte "*Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y El Caribe*" de 2021. A esa conclusión se llegó mediante la aplicación al país del *Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones*[1] ("CCM" por sus

[1] El modelo puede ser consultado en: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

siglas en inglés) del Centro Global de Capacidad en Seguridad Cibernética (GSCC) de la Universidad de Oxford.

Según este modelo, reconocido internacionalmente, cada nivel de madurez es evaluado a partir de cinco dimensiones en las que se examinan aspectos diversos de la ciberseguridad: a) política y estrategia de ciberseguridad, b) cultura cibernética y sociedad, c) educación, capacitación y habilidades en ciberseguridad, d) marcos legales y regulatorios y e) estándares, organizaciones y tecnologías. Cada dimensión comprende una serie de factores a través de los cuales se evalúa la capacidad de generar seguridad cibernética y determinan los aspectos de mejora para incrementar el nivel de madurez.

El estudio del BID y la OEA demuestra que en lo relativo a regulaciones sobre gestión de la seguridad de la información y requerimientos de ciberseguridad, el país está en etapa apenas formativa. Por otro lado, respecto a protección de infraestructuras críticas de información, defensa y ciberseguridad nacional, así como manejo de crisis, el estudio refleja que Costa Rica está en fase incipiente, es decir, no hay madurez del todo o es apenas originaria. En cuanto a respuesta a incidentes, apenas se ha avanzado a una etapa formativa, es decir, esfuerzos coyunturales o desorganizados, especialmente a través de la labor del Centro de respuesta de incidentes de seguridad informática (CSIRT) que, si bien ha sido positiva, fue conceptualizada con una visión limitada desde su inicio, y no tiene el apoyo, ni los recursos necesarios para efectuar su labor, ni brindar la respuesta especializada.

En suma, Costa Rica se encuentra en una etapa entre incipiente y formativa, presenta una madurez embrionaria, donde si bien hay evidencia de los esfuerzos realizados en la materia y se cuenta con iniciativas que se están ejecutando, no hay una verdadera coordinación a nivel nacional ni planeación estratégica, hay una visión limitada sobre lo que implica la ciberseguridad, existe una ausencia

importante de recursos, y no se han tomado suficientes decisiones sobre los beneficios y la necesidad de priorizar la ciberseguridad.

Si bien es cierto, que el país ha avanzado en la materia, lo que se refleja en algunos rankings internacionales, como el Índice Global de Ciberseguridad (GCI, por sus siglas en inglés) de la Unión Internacional de Telecomunicaciones (UIT) del año 2020, el país se ubicó en la posición 76 con un puntaje de 67.45, mostrando una mejora significativa con respecto a lo reportado para el año 2019, cuando el país se encontraba en la posición 115. Sin embargo, también es cierto que, en la práctica, las medidas que han permitido al país avanzar en dichos rankings no se han traducido en acciones efectivas o de impacto en la protección de las bases de datos de todas instituciones que conforman el Estado. De hecho, otros rankings internacionales de renombre, como el "*National Cibersecurity Index*" de Estonia, calificó negativamente al país al pasarlo del puesto 48 en el año 2020, al puesto 60 para este año 2022. En su análisis, este índice revela el pobre desarrollo del país en materia de protección a infraestructura crítica y servicios esenciales, análisis e información de ciberamenazas, y atención de crisis.

Pero la prueba más fehaciente de las carencias del país en este tema, son los ataques cibernéticos significativos que sufrió la administración pública durante los meses de abril, mayo y junio de este año 2022, a casi una treintena de instituciones públicas, esta situación provocó una declaratoria de emergencia nacional de parte del Poder Ejecutivo, que en ningún otro país en la región se había dado.

Estos actos fueron dirigidos contra infraestructuras críticas como los sistemas del Ministerio de Hacienda o de la Caja Costarricense del Seguro Social, incluyendo a otras instituciones como el Instituto Meteorológico Nacional, Radiográfica Costarricense, Ministerio de Trabajo, Ministerio de Ciencia, Tecnología, Innovación y Telecomunicaciones (MICITT), Fondo de Desarrollo Social y Asignaciones Familiares (FODESAF) y la Junta Administrativa del Servicio Eléctrico Municipal de

Cartago (JASEC), entre otras, comprometiendo con ello la prestación de servicios esenciales para la población.

También, la crisis generada por estos ataques obligó a suspender y dar de baja los sistemas informáticos que soportan la prestación de otros servicios y el cumplimiento de obligaciones a cargo del Estado. En el caso del Ministerio de Educación, por ejemplo, la suspensión del sistema “Integra 2”, aparentemente habría generado dificultades para el pago de los salarios de 13 mil funcionarios de esa institución, afectándose con ello los ingresos de las familias que dependen de esos pagos.

Si bien el riesgo de un ataque de este tipo no tiene una probabilidad a cero de que ocurra, lo cierto es que los incidentes comentados dejaron al desnudo la poca o nula preparación del país para gestionar y atender crisis e incidentes de esta magnitud. También revelaron lo desprotegida que se encuentra la infraestructura crítica del país, las nulas responsabilidades que se exigen a los operadores de esas infraestructuras y la poca claridad sobre la institucionalidad a cargo de la coordinación de la ciberseguridad nacional.

Los ciberataques sufridos en Costa Rica han dejado, y siguen acumulando, daños y pérdidas económicas, sociales, y de toda índole, que deberán ser calculadas por las autoridades correspondientes, pero que sin duda alcanzarán cifras millonarias, datos del periódico La República, en su nota publicada el día 20 de abril del 2022, indica que sólo en las primeras 48 horas de hackeo en los sistemas de aduanas del Ministerio de Hacienda, provocaron pérdidas que rondan los $125 millones, según datos de la Cámara de Comercio Exterior (Crecex), la CCSS reporto afectación de entre 30 y 1500 de sus servidores y el pasado lunes 22 de agosto Noticias Repretel, anunciaba que el país estaría expuesto a 35 ataques cibernéticos en los próximos 4 meses del año.

Una de las causas de que los ataques hayan tenido un impacto tan significativo en la continuidad de los servicios prestados por el Estado es la ausencia de inversión y el no haber destinado suficientes recursos a la protección cibernética de nuestras infraestructuras críticas en los últimos años, lo que quedó evidenciado al verse el país en una emergencia tecnológica que lo hizo retroceder 10 años en el avance que se habría logrado en materia de digitalización.

A estos hechos se aúnan los informes de la Contraloría General de la República que han dejado en evidencia la ausencia de una adecuada gestión del riesgo y de la seguridad de la información en las instituciones. En esa línea se pueden mencionar sus Informes DFOE-SAF-IF-00009-2019 y DFOE-BIS-IF-00002-2022, que detectaron vulnerabilidades serias en la gestión de la seguridad de la información del Ministerio de Hacienda y del EDUS (CCSS), precisamente dos de las entidades más afectadas con los hakeos.

Adicionalmente, la Contraloría General de la República ha encontrado deficiencias importantes en la implementación de procesos de gestión de seguridad de la información en el sector público, así como ausencia de personal capacitado en ciberseguridad. Al respecto, en su Informe de Seguimiento de la Gestión Pública No. DFOE-CAP-SGP-00002-2021 de agosto del año 2021, la CGR advirtió que: *"…**el 34% de las instituciones tienen un bajo nivel de implementación del proceso de gestión de seguridad de la información y el 55% no cuentan con personal dedicado a esta labor. Además, el 45% no cuenta con un proceso de gestión de la ciberseguridad de la información y el 62% no cuentan con personal dedicado en esta especialidad".*** (lo subrayado y en negrita no es del original)

Valga destacar, como se menciona más adelante, que Costa Rica no cuenta con regulaciones mínimas, a nivel de Ley, sobre gestión de seguridad informática en el sector público. El ente contralor también, identificó que entre el 2017-2021 se había

presupuestado para las partidas de TI incluyéndose Ciberseguridad un monto por ¢1.296.044.440.250,93 y para el año 2021 se destinaron ¢34.297.314.423,45.

En síntesis, el país está viviendo las consecuencias de no haber invertido en la prevención, educación y la creación del marco regulatorio aplicable para cumplir con la protección de la ciberseguridad a lo largo de los años y de no haberle dado prioridad a un asunto no solo que es crítico, sino de seguridad informática.

Para la elaboración del Proyecto, se ha tomado en consideración el estado de situación de la ciberseguridad en Costa Rica, el marco constitucional y legal del país, la estructura institucional y competencias de las diferentes entidades que componen la administración pública costarricense, y el conocimiento y experiencia de reconocidos expertos en el área que han apoyado técnicamente su redacción.

Por eso con el presente proyecto de ley se pretende posicionar a la ciberseguridad como una prioridad y una política de Estado, la inversión que se requerirá para la puesta en práctica de la iniciativa, no será superior, a los daños generados durante este año y los que podrían generar futuros ciberataques contra la seguridad tecnológica y la soberanía nacional.

En términos generales, el proyecto de ley tiene como finalidad establecer las reglas, la gobernanza e institucionalidad necesarias para proteger, mediante componentes preventivos, reactivos y proactivos, las infraestructuras críticas de información del país y, con ello, la seguridad nacional. El Capítulo I contiene precisamente las finalidades específicas, las definiciones y los principios que rigen la ley, dentro de los cuales destaca el de seguridad por diseño, resiliencia, y el de colaboración y cooperación.

En el Capítulo II, se crea una Agencia Nacional de Ciberseguridad dentro del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), por lo que no se estaría creando un órgano nuevo dentro de la Administración del

Estado costarricense, esto con la finalidad de no hacer más grande el Estado costarricense sino reorganizarlo. El estar inscrita al MICITT no es casualidad, este órgano ha venido desempeñando competencias en materia de ciberseguridad, como la existencia de un CSIRT creado por Decreto Ejecutivo N°37052-MICIT del 09 de marzo del 2012, pero es momento de fortalecerlo, dándole recursos ya existentes en el Estado costarricense pero que están dispersos, se puede realizar una buena gestión canalizándolos hacia este Ministerio que actualmente no posee los insumos, y un marco normativo robusto, en el cual se puedan también generar sanciones por no acatar las indicaciones de la Agencia, en respuesta a la defensa nacional, desde el punto de vista tecnológico.

La Agencia será la responsable de elaborar y ejecutar la política, los Planes Nacionales y la Estrategia Nacional de Ciberseguridad. Además, funcionará como un centro de operaciones de seguridad tecnológica ("G-SOC"2) y estará encargada de coordinar todo lo relativo a la ciberseguridad y protección de infraestructuras críticas del país. La Agencia tendrá tres unidades operativas, encargadas cada una de ellas, de la función preventiva (monitoreo continuo de redes y correlación de datos provenientes de diversos sensores de seguridad digital con especial énfasis en infraestructuras críticas de información), reactiva (respuesta y manejo de alertas e incidentes cibernéticos) y proactiva (inteligencia de datos y predicción de amenazas). En este mismo apartado se establecen las reglas de coordinación y delimitación de competencias de la Agencia con los **reguladores sectoriales**, quienes serán los encargados de supervisar el cumplimiento de la ley por parte de los operadores de infraestructura crítica pertenecientes a esos sectores.

El **Capítulo III**, por su parte, regula el régimen de protección de las **infraestructuras críticas de información ("ICI")**. Se declaran de interés público todas las políticas y acciones relacionadas con la protección de las ICI y **se declaran como amenaza a la seguridad nacional todos los incidentes dirigidos a dichas**

[2] El término "G-SOC" hace alusión a lo que en inglés se denomina un "Government Security Operations Center" ó, en español, un Centro de Operaciones de Seguridad de Gobierno.

**infraestructuras**. Se establecen los criterios para que una infraestructura informática -sea un sistema, red o activo- se considere crítica, por ejemplo, cuando sea necesaria para proveer un servicio esencial y un incidente de ciberseguridad pueda comprometer o interrumpir la prestación de ese servicio.

Como parte de una sección tercera de ese capítulo se disponen las obligaciones que deberán cumplir los operadores de infraestructuras críticas de información. Destacan las obligaciones de reportar todo incidente de ciberseguridad significativo, establecer un sistema de gestión del riesgo, planes de contingencia y continuidad operacional, así como realizar auditorías, evaluaciones de riesgo y ejercicios o test de ciberseguridad periódicos.

El **Capítulo IV** describe los tipos de información que se considerarán confidenciales y la manera de equilibrar la confidencialidad con el derecho de acceso a la información pública, siempre que la revelación de la información específica de que se trate no comprometa la seguridad nacional, ni el interés público, ni tampoco violente la protección a los datos personales o sensibles.

El **Capítulo V** establece las obligaciones mínimas de gestión de la seguridad de la información que deberán cumplir todas las instituciones del sector público. Este capítulo obedece a que en Costa Rica **no existen disposiciones legales sobre seguridad de la información en el sector público**. Por lo tanto, los marcos de gestión de seguridad de la información no están estandarizados a nivel público, favoreciendo la fragmentación y las vulnerabilidades cibernéticas. En esa línea, lo que existía era una norma técnica dictada por la CGR en el año 2007 sobre gestión de sistemas de TI (N-2-2007-CO-DFOE), dictada al amparo de una interpretación extensiva del artículo 16 de la Ley de Control Interno (único que refiere específicamente a sistemas de información), y que fueron derogadas por la CGR en el año 2020 (R-DC-17-2020). Mas recientemente, en el año 2021, el MICITT adoptó unas “Normas técnicas para la gestión y el control de las Tecnologías de

Información” que, nuevamente, sobre gestión de la seguridad de la información lo que contiene es media página con alusiones generales.

En el **Capítulo VI** se establecen las infracciones y sanciones por el incumplimiento a la Ley y en el **Capítulo VII** las obligaciones de coordinación e información con las autoridades judiciales.

Finalmente, se prevén **Transitorios** con el propósito de que las instituciones y actores afectados puedan adaptarse con tiempo a la nueva ley. Además, se prevé un plazo de un año a partir de la entrada en vigor de la Ley (es decir, un año en total desde su aprobación) para que las unidades operativas de la Agencia se constituyan de forma paulatina, conforme se van asignando los recursos y capacidades para ello.

En síntesis, este es un proyecto país necesario, robusto y técnicamente sustentado que, de aprobarse, sería pionero en la región. Pero sobretodo, permitiría al país adentrarse en la Cuarta Revolución Industrial con la preparación necesaria, y de forma comprometida con la seguridad, las necesidades y los derechos de la población. Es una legislación que responde al contexto histórico en el que se enmarca, en donde si en el futuro el país vuelve a sucumbir a un ataque cibernético, será por negligencia de quienes no hayan aprendido las lecciones recientes.

Con fundamento en las consideraciones expuestas, se somete a conocimiento de las señoras y señores Diputados, el presente proyecto de ley.

**LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA**
**DECRETA:**

## “LEY DE CIBERSEGURIDAD DE COSTA RICA “

## CAPÍTULO I

## OBJETO, ÁMBITO DE APLICACIÓN, PRINCIPIOS, Y DEFINICIONES

### ARTICULO 1.- Objeto y fines

Esta ley tiene como objeto crear el marco jurídico para la regulación, el resguardo y protección de la seguridad cibernética de las infraestructuras de tecnologías criticas del país, en la Administración Pública, así como establecer las acciones, requerimientos y la gobernanza necesarios para:

a) Consolidar una política transversal y una estrategia nacional de ciberseguridad que identifique los ejes estratégicos y unifique los esfuerzos del país en esta materia.
b) Proteger la disponibilidad, integridad y confidencialidad de los sistemas de información, las redes y los datos que se generan, almacenan y transmiten por dichos sistemas y redes de todos los habitantes del país;
c) Coordinar la atención y respuesta a los incidentes de ciberseguridad que afecten al sector público y a las infraestructuras críticas de información;
d) Incrementar la resiliencia de las organizaciones públicas del país y de los operadores de infraestructuras críticas de información, frente a las amenazas e incidentes de seguridad del ciberespacio.
e) Gestionar y mitigar de forma adecuada los riesgos de seguridad de los sistemas de información, redes y activos informáticos;

f) Promover la coordinación, cooperación, inteligencia y el intercambio seguro de información relevante sobre amenazas cibernéticas y ciberseguridad, entre las instituciones del Estado, los distintos sectores de la sociedad y organismos internacionales; y
g) Garantizar la seguridad cibernética, asegurar la soberanía del ciberespacio, la seguridad nacional y los intereses públicos, proteger los derechos e intereses legítimos de los ciudadanos, las personas jurídicas y otras organizaciones, y promover el sano desarrollo de la tecnología de la información en los sectores económico y social.

**ARTICULO 2.- Principios rectores**

La aplicación de la presente Ley y, en general, la gestión de la ciberseguridad del país se guiará por los siguientes principios rectores:

1. **Seguridad por diseño**: Todas las partes interesadas deben aplicar un enfoque de seguridad por diseño en el desarrollo, compra o aprovisionamiento de sistemas o recursos informáticos y en los procesos de gestión de los mismos, de manera que la ciberseguridad sea un componente originario, transversal y permanente en la cadena de valor y durante la operación o utilización de los sistemas.

2. **Cooperación.** Todas las partes interesadas deben cooperar, incluso a nivel regional e internacional en la prevención de amenazas del ciberespacio. La cooperación debe tener lugar dentro de los gobiernos, dentro de las organizaciones públicas y privadas, así como entre ellos y con los individuos.

3. **Resiliencia y Continuidad:** las partes interesadas deben ser resilientes para reducir los efectos adversos de los incidentes de ciberseguridad o inseguridad tecnológica, recuperarse en el menor plazo posible y apoyar la continuidad y resistencia de las actividades críticas que dependen de los sistemas de información comprometidos.

4. **Concientización, educación y empoderamiento.** Todas las partes interesadas deben interiorizar el riesgo de ciberseguridad y cómo gestionarlo. Deben ser conscientes de que el riesgo de seguridad digital puede afectar a la consecución de sus objetivos económicos y sociales y puede afectar a terceros. Deben estar dotadas de la educación y las competencias necesarias para comprender este riesgo y ayudar a gestionarlo, así como para evaluar el impacto potencial de sus decisiones.

5. **Responsabilidad.** Todas las partes interesadas deben asumir la responsabilidad de la gestión de los riesgos de ciberseguridad. Deben actuar de forma responsable y rendir cuentas.

6. **Derechos humanos y valores fundamentales.** Todas las partes interesadas deben gestionar el riesgo de ciberseguridad de forma transparente y coherente con los derechos humanos y los valores fundamentales del Estado costarricense.

**ARTICULO 3.- Definiciones**

Para efectos de esta Ley, se entenderá por:

a) Agencia: La Agencia Nacional de Ciberseguridad.

b) Autoridades de Control: La Agencia Nacional de Ciberseguridad o el Regulador Sectorial competente, según sea el caso.

c) Ciberespacio: Dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información, los datos (almacenados, procesados o transmitidos) que abarcan los dominios: físico, virtual y cognitivo; y las interacciones sociales que se verifican en su interior. Las infraestructuras

tecnológicas corresponden a los equipos materiales empleados para la transmisión de las comunicaciones, tales como enlaces, enrutadores, conmutadores, estaciones, sistemas radiantes, nodos, conductores, entre otros. Los componentes lógicos de la información, en tanto, son los diferentes softwares que permiten el funcionamiento, administración y uso de la red.

d) Ciberseguridad: el conjunto de acciones destinadas al estudio y manejo de las amenazas, riesgos e incidentes propios del ciberespacio; a la prevención, mitigación, respuesta y recuperación frente a estos, así como para reducir sus efectos y el daño causado, antes, durante y después de su ocurrencia.

e) Centros de respuesta a incidentes de seguridad informática (CSIRT): Centros conformados por especialistas multidisciplinarios capacitados para gestionar y responder a incidentes de ciberseguridad, en forma rápida y efectiva, y que actúan según procedimientos y políticas predefinidas, coadyuvando asimismo a mitigar sus efectos.

f) Control de seguridad: los controles de gestión, operativos y técnicos utilizados para proteger contra un esfuerzo no autorizado que afecte negativamente a la confidencialidad, integridad y disponibilidad de un sistema de información o de su información.

g) Dato: representación simbólica y desorganizada de un evento único registrado por un sistema digital que se puede procesar, almacenar o trasladar por una red informática.

h) Estándares de Ciberseguridad o Estándares de Seguridad de la Información: Corresponden al conjunto de reglas y procedimientos técnicos básicos sobre ciberseguridad o seguridad de la información, promulgados por la Agencia, y que deberán cumplir las instituciones públicas y/o los operadores de infraestructura crítica.

i) Gestión de incidente de Ciberseguridad: Conjunto ordenado de acciones enfocadas a prevenir, en la medida de lo posible, la ocurrencia de incidentes de ciberseguridad y, en caso de que ocurran, atender el incidente y restaurar los niveles de operación lo antes posible.

j) Incidente de Ciberseguridad: Todo evento o acción no autorizada que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados en dichos sistemas, o de los servicios correspondientes ofrecidos a través de sistemas informáticos o redes de telecomunicaciones, que puedan afectar al normal funcionamiento de los mismos. Se utilizarán como sinónimos de este concepto, el de incidente o ataque cibernético, ciberataque, brecha de seguridad, entre otros similares.

k) Información: representación de un conjunto de datos organizado mediante reglas definidas que permiten identificar e interpretar las características de un sujeto o un objeto mediante el uso de tecnología digital.

l) Infraestructura Crítica de Información (ICI): Todo sistema informático, dispositivo, equipo, red y, en general, infraestructura o activo informático declarado como tal en los términos de esta ley.

m) Operador de infraestructuras críticas de información: Toda persona física o jurídica, pública o privada, que, por sí o de forma conjunta con otra, ejerza el control efectivo sobre una infraestructura crítica de información, independientemente del título o causa por la cual ejerza dicho control.

n) Regulador sectorial: Entidad pública dentro de cuyas funciones principales se encuentra la regulación y/o supervisión de uno o más sectores regulados específicos.

o) Resiliencia: Capacidad de las redes o sistemas de información para seguir operando pese a estar sometidos a un incidente de ciberseguridad o ciberataque, aunque sea en un estado degradado, debilitado o segmentado; y, también, la capacidad de restaurar con presteza sus funciones esenciales después de un incidente de ciberseguridad o ciberataque, por lo general con un efecto reconocible mínimo.

p) Riesgo: Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y/o sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto negativo en éstas.

q) Sector regulado: Sector que representa alguna actividad económica estratégica para el país, que se encuentra sometido a la supervisión de un regulador o fiscalizador sectorial.

r) Servicios esenciales: Todo servicio, prestado por el Estado o por empresas privadas, respecto del cual la afectación, degradación, denegación de servicio, interceptación, interrupción, no disponibilidad o destrucción de su infraestructura de la información pueda afectar gravemente: la vida o integridad física de las personas; la provisión de servicios sanitarios, de seguridad, energéticos, de suministro de agua o de telecomunicaciones; y al normal funcionamiento de infraestructura vial y medios de transporte; a la generalidad de usuarios o clientes de sistemas necesarios para operaciones financieras, bancarias, de medios de pago y/o que permitan la transacción de dinero o valores; o de modo general, el normal desarrollo y bienestar de la población.

Se considerarán servicios esenciales, para efectos de esta Ley, los servicios declarados como servicios públicos en el artículo 5 de la Ley Nº 7593, Ley de la Autoridad Reguladora de los Servicios Públicos (ARESEP).

s) Sistema informático o Sistema de información: Todo sistema, dispositivo, equipo, red o activo aislado o el conjunto de ellos, interconectados o relacionados entre sí, incluidos sus soportes lógicos, cuya función, o la de alguno de sus elementos, sea la recogida, el almacenamiento, la utilización, el intercambio, la difusión, la transmisión, la eliminación o, en general, el tratamiento de información, en ejecución de un programa.

t) Vulnerabilidad de seguridad: cualquier atributo del hardware, el software, el proceso o el procedimiento que podría permitir o facilitar la anulación o evasión de un control de seguridad.

## CAPÍTULO II

## CREACIÓN DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD

**ARTICULO 4.- De la naturaleza jurídica y composición de la Agencia Nacional de Ciberseguridad (ANC)**

1. Créase la Agencia Nacional de Ciberseguridad como un órgano adscrito al Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) con independencia técnica para velar por el cumplimiento y ejecución de la presente Ley.

2. La Agencia Nacional de Ciberseguridad fungirá como el Centro de Operaciones de Ciberseguridad (“SOC”) del país, encargado de la gestión preventiva, reactiva y proactiva de las amenazas e incidentes que, a través del uso de datos, puedan generar un riesgo de seguridad para la población costarricense.

3. La Agencia estará conformada, por una Dirección General que la dirigirá, con apoyo de un Consejo Asesor, y las siguientes tres unidades operativas independientes entre sí:

a) El Centro de Intercambio y Monitoreo de Redes (CIMR-CR), que tendrá a su cargo la función preventiva y monitoreo continuo de alertas provenientes de los dispositivos del entorno, así como la responsabilidad de correlacionar, analizar y reportar todo patrón de riesgo identificado durante el monitoreo de amenazas y vulnerabilidades. Tiene a su cargo garantizar la ingesta permanente de datos del entorno provenientes de los sensores de seguridad en conjunto con las organizaciones y sus proveedores.

b) El Centro de Respuesta a Incidentes de Seguridad (CSIRT-CR), que tendrá a su cargo la función reactiva, consistente en gestionar los canales de comunicación para la recepción de alertas informáticas, realizar la clasificación de dichas alertas, mantener el registro de incidentes creado en esta ley y el nivel de riesgo actualizados, así como la responsabilidad de investigar y proveer soporte a las instituciones afectadas por algún incidente que así lo requieran, emitir los boletines de alerta y generar las campañas de concientización en ciberseguridad.

c) El Centro de Inteligencia de Datos en Ciberseguridad (CID-CR), que tendrá a su cargo la función proactiva, consistente en proporcionar datos e información predictiva a la Agencia para facilitar la toma de decisiones, asegurar el cumplimiento de las misiones y objetivos a largo plazo, reducir la superficie de ataque, crear ejercicios de simulación de amenazas y modelado de adversarios, así como mantener a la Agencia y quienes utilicen sus servicios permanentemente actualizados en nuevas amenazas del entorno nacional e internacional.

4. Sin perjuicio de lo establecido en el artículo 11 para el CSIRT-CR, el Reglamento a esta Ley especificará y delimitará las funciones de cada una de estas unidades operativas, en armonía con la función principal que se les atribuye en este artículo. En caso de conflicto, el Director de la Agencia delimitará las

competencias. El Reglamento a esta ley dispondrá la forma de organización de dichas unidades.

**ARTICULO 5.- Atribuciones y Patrimonio de la Agencia Nacional de Ciberseguridad**

1. La Agencia Nacional de Ciberseguridad tendrá las siguientes atribuciones:
   a) Definir y gestionar la Política Nacional de Ciberseguridad de mediano plazo.

   b) Coordinar todas las acciones relacionadas con ciberseguridad en la Administración Pública y servir como Centro de Operaciones de Ciberseguridad (“SOC”) de la Nación.

   c) Asegurar la continuidad y resiliencia de las infraestructuras críticas de información del país, así como ggarantizar la seguridad cibernética, asegurar la soberanía del ciberespacio, la seguridad nacional y los intereses públicos, proteger los derechos e intereses legítimos de los ciudadanos, las personas jurídicas y otras organizaciones, y promover el sano desarrollo de la tecnología de la información en los sectores económico y social.

   d) Elaborar, definir y actualizar la Estrategia Nacional de Ciberseguridad, así como coordinar y dar seguimiento a los planes de acción para su debida ejecución y cumplimiento.

   e) Identificar y designar, con el apoyo del Consejo Asesor, las infraestructuras críticas de información en la forma establecida en el artículo 16 de esta Ley y su reglamento.

   f) Supervisar a los operadores de infraestructuras críticas de información en el cumplimiento de la presente Ley, salvo en sectores regulados sujetos a supervisión de un regulador sectorial, en los términos del artículo 11 de esta Ley.

g) Dictar y aprobar normas técnicas de carácter general para garantizar la unidad de acción estatal en materia de ciberseguridad y la debida aplicación de la presente ley.

h) Aprobar estándares mínimos de ciberseguridad o seguridad de la información, internacionalmente reconocidos, que deba adoptar la Administración Pública en sentido amplio, y los operadores de infraestructuras críticas de información

i) Girar instrucciones vinculantes a los operadores privados de infraestructura crítica de información que no se encuentren sometidos a la regulación o fiscalización de un regulador o fiscalizador sectorial, y a los órganos o entidades públicas pertenecientes al Poder Ejecutivo, dentro del campo de las competencias previstas en esta Ley.

j) Proponer, con la asesoría del Consejo Asesor, un Plan Nacional de Contingencia para Emergencias y Crisis de Ciberseguridad será el plan a utilizar en caso de emergencias decretadas por motivos de ciberseguridad. Este Plan deberá ser aprobado por la Junta Directiva de la Comisión Nacional de Emergencias mediante el procedimiento previsto en la Ley Nacional de Emergencias y Prevención del Riesgo, Nº 8488.

k) Proponer al jerarca del MICITT las normas legales y reglamentarias que se requieran para asegurar el acceso seguro al ciberespacio, así como aquellas que estén dentro del marco de su competencia.

l) Coordinar con los reguladores sectoriales competentes, con los CSIRT o Centros de Operaciones sectoriales, si los hubiese, con los operadores de infraestructuras críticas nacionales e instituciones públicas, según corresponda, en la prevención, detección, investigación y respuesta a vulnerabilidades, amenazas e incidentes de ciberseguridad.

m) Administrar el Registro Nacional de Incidentes de Ciberseguridad, y establecer indicadores de estado o nivel de alerta públicos.

n) Requerir de los CSIRT Sectoriales, de los reguladores sectoriales, de los operadores de infraestructura crítica, y de las instituciones públicas, la información para el cumplimiento de sus fines.

o) Diseñar e implementar, junto con los distintos sectores de la sociedad, planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad.

p) Recomendar al jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), la celebración de convenios, y cooperar con organismos públicos, entidades privadas, academia, organizaciones internacionales u organizaciones no gubernamentales, destinados a facilitar la formación, la colaboración y la transferencia de información y conocimiento que permita el cumplimiento de los fines de esta Ley.

q) Prestar asesoría técnica a instituciones públicas en general y a las entidades privadas que sean operadores de infraestructura crítica de información, que así lo requieran o que estén o se hayan visto afectados por un incidente de ciberseguridad.

r) Colaborar y coordinar con centros de operaciones de seguridad, centros de respuesta a incidentes, organismos de inteligencia y seguridad nacional e investigación judicial, nacionales e internacionales, para enfrentar amenazas que puedan afectar a la infraestructura crítica de información e implementar acciones preventivas.

s) Adoptar y publicar guías de mejores prácticas o manuales en materia de ciberseguridad para orientar el cumplimiento de la ley.

t) Velar por el cumplimiento de esta ley, sus reglamentos y la normativa técnica que se dicte en conformidad con la presente ley, cuando ello no corresponda a un regulador o fiscalizador sectorial.

u) Representar al Gobierno en cuestiones de ciberseguridad a nivel nacional e internacional.

v) Denunciar ante las autoridades competentes la posible comisión de delitos cibernéticos.

w) Realizar todas aquellas otras funciones que las leyes le encomienden.

2. Los recursos de la Agencia serán los siguientes:

a) Un 1.5% del total de recursos presupuestados por todas las instituciones del Sector Público, que deberán ser transferidos a la Agencia antes del 30 de enero de cada ejercicio presupuestario. Las instituciones transfirientes deberán cumplir con lo dispuesto en el título IV de la Ley N° 9635. Aquellas de estas que no trasladen los recursos en la cantidad y el plazo definido en la presente ley, no podrán asignar presupuestariamente en el siguiente ejercicio económico un monto superior al gasto ejecutado en el año precedente según la liquidación respectiva, hasta tanto se realicen las transferencias adeudadas.

b) Las donaciones y las subvenciones provenientes de otros países, entidades públicas u organismos internacionales, que no comprometen la independencia y la transparencia de la Agencia, en los términos que establezca el reglamento.

c) Los recursos que se obtengan, serán utilizados para el cumplimiento de los objetivos de esta Ley y para fortalecer, desarrollar, actualizar y mejorar a la Agencia.

d) Los ingresos por el cobro de las multas previstas en esta Ley. En el caso de multas aplicadas por los reguladores sectoriales competentes, un 50% de lo recolectado deberá ser transferido a la Agencia.

Se autoriza a las instituciones del Estado y entidades públicas estatales para que asignen y realicen convenios para dotar del personal calificado a la Agencia para cumplir sus fines, funciones y ejecutar proyectos específicos. En tales casos aplicarán las mismas restricciones indicadas en el inciso b) de este artículo.

**ARTICULO 6.- De la Dirección Nacional**

La dirección y administración superior de la Agencia estará a cargo de un Director Nacional, quién será designado por el Poder Ejecutivo mediante concurso público, previa demostración de idoneidad. El nombramiento se efectuará por un periodo de cinco años, prorrogable por otro periodo igual consecutivo.

La persona directora deberá poseer:

1. Título académico que la acredite como profesional en ingeniería en sistemas o en sistemas informáticos o similar.
2. Tener al menos ocho años de experiencia en temas de ciberseguridad.
3. Contar con atestados comprobados, estudios y certificaciones que la acrediten como experta o experto en materia de ciberseguridad o seguridad informática.

La persona directora solo puede ser cesada antes del vencimiento de su cargo, por renuncia expresa, o por decisión del Poder Ejecutivo debidamente motivada y cumpliendo el debido proceso, además, de las siguientes causales:

a. Incumplimiento grave y demostrado de sus obligaciones;

b. Incapacidad física o cognitiva sobrevenida para el ejercicio de su función;

c. Incompatibilidad grave por hechos sobrevenidos que impidan o dificulten que pueda ejercer las funciones atribuidas en esta Ley de forma imparcial e independiente, y en cumplimiento del interés público; o

d. Condena firme por delito doloso.

La remoción de la persona Directora deberá tramitarse mediante el procedimiento ordinario establecido en la Ley N.º 6227, Ley General de la Administración Pública, del 2 de mayo de 1978 y sus reglamentos. En el caso de los supuestos a) y c) anteriores, una vez tramitado el procedimiento, pero de previo a la adopción de la resolución final que decida sobre la separación, el Poder Ejecutivo enviará a la Procuraduría General de la República el expediente, para que ésta se manifieste, en un plazo razonable, sobre el carácter “grave” de la falta o la incompatibilidad y la procedencia de la separación. El criterio de la Procuraduría no será vinculante pero el Poder Ejecutivo deberá motivar su decisión de separarse de dicho criterio, si fuera el caso.

**ARTICULO 7.- Atribuciones de la Dirección Nacional**

Corresponderá a la Dirección Nacional:

a) Elaborar la propuesta de política nacional de ciberseguridad de mediano plazo, y las modificaciones que se requieran. Dicha propuesta será sometida a aprobación conjunta de los Ministros de Seguridad Pública, Ciencia y Tecnología y Presidencia, ante solicitud del Director Nacional.

b) Planificar, organizar, dirigir, coordinar y controlar el funcionamiento de la Agencia;

c) Dirigir, coordinar y asignar labores y funciones de las unidades operativas de la Agencia.

d) Dictar las resoluciones y demás actos administrativos necesarios para el buen funcionamiento de la Agencia;

e) Emitir resoluciones, normativa y lineamientos generales que de acuerdo con esta ley corresponda dictar a la Agencia;

f) Promulgar los estándares técnicos en materia de ciberseguridad que dispone esta ley;

g) Ejecutar los actos y celebrar los convenios necesarios para el cumplimiento de los fines de la Agencia.

h) Delegar atribuciones o facultades específicas en funcionarios de los ámbitos profesionales o técnicos de la Agencia;

i) Comunicar a las instituciones u autoridades competentes cualquier incumplimiento o potencial incumplimiento a esta ley que la Agencia o el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) no tenga competencia para sancionar.

j) Todas las demás funciones que otorgue esta u otras leyes a la Agencia

**ARTICULO 8.- Del Consejo Asesor en Ciberseguridad**

La Agencia contará con un Consejo Asesor en Ciberseguridad, constituido por los siguientes miembros:

a) El Director de la Agecia, quien lo presidirá.

b) Un representante del Consejo de la Superintendencia de Telecomunicaciones;

c) Un representante de la Junta Directiva de la Autoridad Reguladora de los Servicios Públicos (ARESEP).
d) Un representante del Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF);

e) El director o directora del Organismo de Investigación Judicial, o su representante;

f) Un representante de la Cámara de Tecnologías de la Información y la Comunicación (CAMTIC);

g) Un representante de la Cámara de Infocomunicación y Tecnología (INFOCOM); y

h) Un representante del Colegio de Profesionales en Informática y Computación.

No podrán formar parte del Consejo quienes tengan un evidente conflicto de interés, en los términos definidos en esta ley.

Los miembros de este Consejo no devengarán dietas.

**ARTICULO 9.- Funciones del Consejo**

Corresponderá al Consejo:

a) Asesorar a la Agencia en materia relacionada con la ciberseguridad y la protección y aseguramiento de la Infraestructura Crítica de la Información para el país;

b) Asesorar en la determinación de los sectores y/o servicios esenciales que posean infraestructura de la información que deba ser calificada como crítica, y a la Agencia en la determinación de los operadores de dichas infraestructuras.

c) Asesorar a la Agencia en las materias que ésta le solicite.

**ARTICULO 10.- Funcionamiento del Consejo**

El Consejo sólo podrá sesionar con la asistencia de al menos, cinco de sus miembros, previa convocatoria del Ministro. Sin perjuicio de lo anterior, el Director estará obligado a convocar a una sesión extraordinaria cuando así lo requieran, por escrito, a lo menos tres de sus miembros. En todo caso, el Consejo podrá autoconvocarse en situaciones urgentes o necesarias conforme a la decisión de la mayoría de sus integrantes y se consignará acta de las sesiones y los acuerdos.

El Reglamento a esta ley determinará las demás normas necesarias para el correcto funcionamiento del Consejo, incompatibilidades, causales de cesión en el cargo y otros.

**ARTICULO 11.- Del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR)**

1. El Centro Nacional de Respuesta a Incidentes de Seguridad Informática (en adelante, “CSIRT-CR”) de la Agencia será el responsable de centralizar, coordinar, respaldar y optimizar los procesos de respuesta y recuperación de incidentes de ciberseguridad generados en las infraestructuras críticas de información y en los sistemas y tecnologías de la información y comunicación de los entes y órganos de la Administración Pública.

2. En el ejercicio de sus funciones, el CSIRT-CR coordinará con los reguladores sectoriales competentes, con los CSIRT sectoriales, con los operadores de infraestructuras críticas y con los demás entes y órganos de la Administración

Pública, así como con organismos o entidades nacionales e internacionales de naturaleza similar.

3. Sin perjuicio de otras que se le asignen vía reglamento, el CSIRT-CR tendrá las siguientes funciones:
   a) Recibir, agregar y analizar los informes relacionados con los incidentes de ciberseguridad significativos (según se establezca de conformidad con en esta ley o su reglamento) recibidos directamente de los operadores de infraestructuras críticas de información, o de los reguladores o CSIRT sectoriales, para mejorar el conocimiento de la situación de las amenazas a la ciberseguridad en todos los sectores de las infraestructuras críticas.

   b) Respaldar, coordinar y apoyar las labores de respuesta y recuperación de amenazas e incidentes de ciberseguridad de los operadores de infraestructuras críticas que no estén sujetos a la supervisión de un regulador sectorial, y los que se presenten en la totalidad de la Administración Pública.
   c) Coordinar y cooperar con los CSIRT o Reguladores Sectoriales frente a ataques, vulnerabilidades, incidentes y brechas de ciberseguridad que afecten a las infraestructuras críticas de información sometidas a supervisión del regulador sectorial. En estos casos, el CSIRT-CR podrá recomendar, colaborar, compartir información, coordinar y realizar todas las acciones conjuntas necesarias para asegurar una respuesta rápida frente al incidente. Además, podrá supervisar la implementación de medidas de mitigación de corto plazo, e informarse de las medidas de largo plazo adoptadas.

   d) Colaborar, cooperar e intercambiar información general y anonimizada sobre amenazas e incidentes de ciberseguridad, con los CSIRT o Centros de Operaciones de Seguridad que se conformen en el sector privado.

   e) Servir de punto de enlace con Equipos de Respuesta a Incidentes de Seguridad Informática extranjeros o sus equivalentes, para el intercambio de

información de ciberseguridad, siempre dentro del marco de sus competencias.

f) Prestar colaboración y asesoría técnica a los CSIRT Sectoriales en la implementación de políticas y acciones relativas a ciberseguridad y ofrecer soporte a los CSIRT Sectoriales o CSIRT internos de los operadores de infraestructuras críticas, para asegurar la resiliencia de los sistemas informáticos en caso de fallas operacionales graves o ciberataques.

g) Consolidar los reportes de incidentes de ciberseguridad que reciba para efectos de la alimentación del registro previsto en el artículo 13.

h) Requerir a los CSIRT Sectoriales o a los operadores de infraestructura crítica, dentro del ámbito de su competencia, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.

i) Crear y administrar para el cumplimiento de sus funciones una plataforma electrónica de comunicaciones segura, destinada a comunicar y compartir información con los otros CSIRT Sectoriales, reguladores sectoriales, operadores de infraestructura crítica y sector privado. El funcionamiento de la red de comunicaciones se establecerá en el reglamento de la presente ley.

**ARTICULO 12.- De los Centros Sectoriales de Respuesta a Incidentes de Seguridad Informática (CSIRT Sectorial)**

1. Los reguladores sectoriales podrán constituir Centros Sectoriales de Respuesta a Incidentes de Ciberseguridad, conocidos como “CSIRT Sectoriales”, los que tendrán por finalidad respaldar la respuesta y recuperación de incidentes de ciberseguridad significativos que pongan en riesgo las infraestructuras críticas de información de sus respectivos sectores regulados. Un reglamento aprobado

por cada uno de dichos reguladores dispondrá la conformación, organización y funciones de su respectivo CSIRT sectorial.

2. Sin perjuicio de otras funciones que se le asignen vía reglamento, corresponderá a los CSIRT Sectoriales, lo siguiente:
   a) Respaldar la respuesta a amenazas e incidentes de ciberseguridad que vulneren o pongan en riesgo las infraestructuras críticas de información de su sector.

   b) Coordinar a los equipos CSIRT internos o departamentos internos de tecnologías de la información de los operadores de infraestructuras críticas de información de su sector, frente a ataques, amenazas, incidentes y brechas de ciberseguridad.

   c) Ofrecer soporte a los CSIRT o departamentos de tecnologías de la información de los operadores regulados para asegurar la resiliencia de estos en caso de fallas operacionales graves, incidentes de ciberseguridad o ciberataques.

   d) Junto al regulador sectorial y/o bajo su supervisión, realizar entrenamiento, educación y capacitación en materia de ciberseguridad, con la finalidad de procurar que los órganos de la Administración de Estado de su sector y de las empresas reguladas cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques.

   e) Requerir a los CSIRT o departamentos de tecnologías de la información de sus operadores regulados, dentro del ámbito de su competencia, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas.

f) Generar y difundir información mediante campañas públicas dentro de su sector.

g) Trabajar coordinadamente con el CSIRT-CR y con otros CSIRT sectoriales, cuando corresponda, en la gestión de un incidente de ciberseguridad.

h) Informar al CSIRT-CR, de vulnerabilidades, incidentes de ciberseguridad y ciberataques detectados o reportados en su sector, junto a sus respectivos cursos o planes de acción para subsanarlos.

i) Prestar asesoría técnica a los operadores de su sector, que estén o se hayan visto afectadas por un incidente de ciberseguridad que haya comprometido su infraestructura crítica de información.

j) Difundir las alertas preventivas e informaciones de ciberseguridad emanadas de la Agencia o de alguna de sus unidades, a los operadores de su sector.

**ARTICULO 13.- Registro Nacional de Incidentes de Ciberseguridad.**

El Registro Nacional de Incidentes de Ciberseguridad, estará a cargo del CSIRT-CR y tendrá carácter público, por exigirlo el debido cumplimiento de las funciones de la Agencia, el debido resguardo de los derechos de las personas y la seguridad de la nación en materia de información crítica. En este registro se ingresarán los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio. Sobre la base de este registro se podrán realizar las respectivas investigaciones por parte del CID-CR, así como las comunicaciones de alertas por parte del CIMR-CR a los CSIRT o Reguladores Sectoriales, a las instituciones públicas y a los operadores de infraestructuras críticas de información.

El reglamento a esta ley establecerá el nivel de prejuicio de datos sensibles del Registro, para garantizar la privacidad de la organización afectada, dependiendo del

estado del incidente y su relación con el criterio de seguridad nacional tecnológica que se aplique, así como las maneras en que dicho registro puede ser consultado por los ciudadanos y otras organizaciones que así lo requieran.

**ARTICULO 14.- Delimitación de Competencias de la Agencia y los Reguladores Sectoriales**

Los reguladores sectoriales serán los competentes para supervisar y verificar el cumplimiento de las disposiciones de la presente Ley y aquellas que emita la Agencia en ejecución de la misma, por parte de los operadores de infraestructuras críticas de información sujetos a su supervisión o regulación. Lo anterior se entenderá sin perjuicio de las potestades de coordinación nacional que posee la Agencia Nacional de Ciberseguridad en todo lo relacionado a la ciberseguridad de la infraestructura crítica de la Nación.

Los reguladores sectoriales podrán dar instrucciones, dictar circulares, órdenes, normas de carácter general y normas técnicas para garantizar un adecuado nivel de ciberseguridad respecto de sus regulados o fiscalizados, de conformidad a la regulación sectorial respectiva, para lo cual considerarán, los lineamientos y normas técnicas generales establecidas en esta ley y por la Agencia Nacional de Ciberseguridad y las demás medidas y obligaciones dispuestas en esta ley.

## CAPÍTULO III
## RÉGIMEN DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN (ICI)

### Sección Primera
### Declaratoria de Interés público y seguridad nacional

**ARTICULO 15.- Declaración de interés público y seguridad nacional**

Por tratarse de activos vitales, críticos y estratégicos para el funcionamiento del Estado y la protección de la vida, la salud, la seguridad y los derechos de la

población, se declaran de interés público nacional todas las políticas y acciones relacionadas con la ciberseguridad de las infraestructuras críticas de información del país. Estas acciones serán dirigidas y coordinadas por el Poder Ejecutivo, a través de la Agencia Nacional de Ciberseguridad, bajo el principio de la unidad de la acción estatal.

Cualquier amenaza o incidente de ciberseguridad que recaiga o esté dirigido a una infraestructura crítica de información o a un sistema estrechamente vinculado con ésta, se considerará una amenaza o atentado contra la seguridad tecnológica nacional.

## Sección Segunda
## Designación de infraestructuras críticas de información

**ARTICULO 16.- Designación de infraestructuras críticas de información**

1. Se considerarán infraestructuras críticas de información todos aquellos sistemas, redes, equipos y, en general, activos e infraestructura informática, física o virtual, que cumplan dos criterios: que sean necesarios para la provisión de servicios esenciales; los sectores o industrias reguladas y/o sus actividades económicas estratégicas; el efectivo cumplimiento de las funciones del Estado; o garantizar la vida, la salud, la seguridad o la economía nacional; y que un incidente de ciberseguridad dirigido a dicha infraestructura o a la organización que la controla, pueda comprometer la prestación continua y de calidad de esos servicios esenciales, afectar el funcionamiento normal del sector o actividad regulada, o poner en riesgo el efectivo cumplimiento de funciones básicas del Estado, así como la vida, la salud, la seguridad o la economía nacional.

2. El Poder Ejecutivo, mediante decreto, especificará cada uno de los sectores, actividades, funciones y servicios comprendidos en el punto anterior y que estarán cubiertos por la regulación de infraestructuras críticas prevista en esta ley. Para ello efectuará un análisis de los riesgos derivados de un eventual incidente en la

prestación o funcionamiento de dichos servicios o sectores, tomando en cuenta, entre otros, las definiciones de servicio esencial y sector regulado contenidas en el artículo 2 de esta ley, así como el criterio de los reguladores sectoriales del país.

3. La Agencia Nacional de Ciberseguridad será la encargada de identificar, a partir de los sectores, actividades, funciones y servicios especificados por el Poder Ejecutivo en el Decreto mencionado en el punto anterior, a los operadores que ejercen el control sobre las infraestructuras críticas de información, excepto en el caso de los operadores pertenecientes a un sector regulado sujeto a supervisión de un regulador sectorial. En este último supuesto, corresponderá a dicho regulador identificar y notificar al operador sobre su designación.

4. En el acto de designación de un operador de infraestructura crítica de información, la Agencia Nacional de Ciberseguridad o el regulador sectorial, según sea el caso, deberá:

a) Identificar al operador del sistema informático, red o activo designado como una infraestructura crítica de información;

b) Identificar, en la medida de lo posible y según las particularidades del caso, el sistema informático, red o activo que se designa como una infraestructura crítica de información;

c) Informar al operador, en términos generales, sobre sus deberes y responsabilidades, en virtud de la presente ley, y que surjan de la designación;

d) Informar al operador de la infraestructura crítica de información sobre su potestad de recurrir la designación, lo cual podrá hacer el operador en un plazo de cinco días hábiles a partir de la notificación del acto administrativo que declare dicha designación.

5. El operador que reciba una designación bajo el presente artículo podrá solicitar a la Agencia o al regulador sectorial, en el plazo de cinco días hábiles, que proceda a modificar o redirigir la notificación, en cuyo caso deberá presentar pruebas de que:

a) El operador no puede cumplir con las obligaciones de la sección tercera de este Capítulo porque no tiene un control efectivo sobre las operaciones del equipo o sistema informático, ni la capacidad o el derecho a realizar cambios en el equipo o sistema informático; y

b) Otra persona física o jurídica tiene el control efectivo sobre las operaciones del sistema informático y la capacidad y el derecho a realizar cambios en el equipo o sistema informático.

**ARTICULO 17.- Requerimientos de información para evaluar los criterios de infraestructura crítica de información**

Cuando la Agencia o el regulador sectorial, según corresponda, tengan razones para inferir que un sistema informático, red o activo informático podría cumplir los criterios de una infraestructura crítica de información, la Agencia o el Regulador podrán solicitar a toda persona u organización que ejerza funciones o control sobre el sistema informático, que le facilite, en un plazo razonable especificado en el requerimiento, la información pertinente y necesaria, relativa a dicho sistema informático, para determinar si el sistema cumple los criterios de una infraestructura crítica de información.

## Sección Tercera
## Obligaciones de los Operadores de Infraestructuras Críticas de Información

**ARTICULO 18.- Obligación general**

Será obligación de los operadores de infraestructuras críticas de información, aplicar las medidas de seguridad tecnológica, organizacionales, físicas, lógicas e informativas necesarias para prevenir, identificar, reportar y resolver incidentes de ciberseguridad y gestionar los riesgos, así, como contener y mitigar el impacto sobre

la continuidad operacional, la confidencialidad de la información y la integridad del servicio prestado, de conformidad a lo prescrito en esta ley, su reglamento y las disposiciones generales emitidas por la Agencia Nacional de Ciberseguridad o el regulador sectorial competente.

**ARTICULO 19.- Obligaciones específicas**

Sin perjuicio de otras obligaciones establecidas en esta ley, los operadores de infraestructuras críticas de información deberán:

a) Reportar a la Agencia o al regulador sectorial, según corresponda, todo incidente de ciberseguridad que afecte su infraestructura crítica de información, en los términos y formas establecidos en el artículo 20 de esta ley.

b) Designar a un Oficial de Respuesta a Incidentes que será el responsable, en nombre del operador, de notificar a la autoridad de control competente sobre el incidente, coordinar su atención a lo interno de la organización, y servir de punto de contacto para recibir comunicaciones y órdenes de parte de dicha autoridad. Si quien controla, administra o aloja la infraestructura afectada es un tercero contratista o proveedor, se podrá designar a dicho tercero como Oficial de Respuesta, sin que ello implique renuncia alguna a la responsabilidad del operador. Si el operador tuviese un CSIRT o un Centro de Operaciones de Seguridad interno, quien coordine dicho equipo o centro será el Oficial de Respuesta a Incidentes. En caso de no designarse expresamente dicho Oficial, el Oficial de Respuesta a Incidentes será la persona que dirija el Departamento de Tecnologías de Información o su homólogo.

c) Implementar un sistema de gestión de riesgo permanente con el fin de identificar aquellos riesgos que pueden afectar la seguridad de los sistemas informáticos, aquellos que afectarían la continuidad operacional del servicio y aquellos que facilitan la ocurrencia de incidentes de ciberseguridad, incluidos los riesgos asociados a la cadena de suministro del operador o a su uso de productos y

servicios de terceros. Dicho sistema debe contar con la capacidad de determinar la gravedad de las consecuencias de un incidente de ciberseguridad.

d) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de riesgos, de conformidad a lo que señale el reglamento a esta ley. Lo anterior incluirá el registro del cumplimiento de la normativa sobre ciberseguridad y del conocimiento por los empleados, dependientes y proveedores, de los protocolos de ciberseguridad y la aplicación de los mismos, tanto durante el funcionamiento regular como en caso de haber sufrido un incidente de ciberseguridad. Sin perjuicio de los planes, procedimientos y estándares obligatorios aplicables a la totalidad de la Administración Pública, dispuestos en el Capítulo V de esta ley, elaborar e implementar planes de ciberseguridad, planes de contingencia, y planes de continuidad operacional. Dichos planes deberán ser actualizados cada año.

e) Realizar continuamente operaciones de revisión, ejercicios, simulacros, test y análisis de las redes, sistemas informáticos, plataformas y sistemas para detectar acciones, vulnerabilidades, omisiones o programas maliciosos que comprometan la ciberseguridad y comunicar los resultados a la Agencia o al regulador sectorial competente.

f) Sin perjuicio de las potestades de investigación, respaldo, y coordinación de la Agencia o el regulador Sectorial, responder a los incidentes de ciberseguridad según sus planes y protocolos internos de ciberseguridad, contingencia y continuidad operacional y adoptar las medidas necesarias para reducir el impacto y la propagación del incidente, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario.

**ARTICULO 20.- Reporte de incidentes de ciberseguridad en infraestructuras críticas de información**

1. El operador de una infraestructura crítica de información deberá reportar mediante un informe dirigido al CSIRT-CR, al CSIRT Sectorial, o al regulador sectorial competente en caso de que no haya CSIRT en dicho sector, según corresponda, la ocurrencia de todo incidente de ciberseguridad que afecte a una infraestructura crítica de información, en cuanto tenga conocimiento de la situación.

2. El informe del incidente debe contener, como mínimo y siempre que las circunstancias lo permitan en ese momento, información sobre:
   a) Una descripción del incidente de ciberseguridad significativo, incluyendo la identificación de los sistemas de información, redes o dispositivos que fueron afectados por dicho incidente, y el rango de fecha estimado de este.

   b) En su caso, una descripción de las vulnerabilidades explotadas y de las defensas de seguridad existentes, así como de las tácticas, técnicas y procedimientos posiblemente utilizados en el incidente.

   c) Una descripción de las medidas tomadas hasta el momento y las que se implementarán a corto plazo.

   d) En su caso, cualquier información de identificación relacionada con el actor que razonablemente se cree que es responsable de dicho incidente.

   e) En su caso, una descripción y, si es posible, cuantificación, de los daños causados, así como la identificación de la categoría o categorías de información a la que se ha accedido o se cree razonablemente que se ha accedido por una persona no autorizada.

   f) Nombre, rol dentro de la organización, e información de contacto del Oficial de Respuesta a Incidentes.

3. El operador deberá presentar actualizaciones periódicas del informe inicial cada vez que se disponga de información nueva o diferente sobre el incidente, hasta la fecha en que la investigación del incidente haya concluido y que el incidente asociado se haya mitigado y resuelto por completo.

4. La Agencia Nacional de Ciberseguridad, en colaboración con el Consejo Asesor, establecerá y publicará, mediante norma técnica general, los criterios para determinar que es un incidente de seguridad

5. El operador de la infraestructura critica deberá notificar a las personas afectadas por los incidentes establecidos en este artículo en caso de que las personas afectadas no pueden ser notificadas individualmente, al público en general, se hará en un plazo de diez días hábiles.

6. En caso de incumplimiento del inciso anterior, la notificación de los incidentes establecidos en este artículo podrá ser realizada por la Agencia, CSIRT-CR, el regulador sectorial competente o, si lo hubiese, el CSIRT sectorial, sin perjuicio de las sanciones que pueda corresponder al operador por dicho incumplimiento. En este caso, la Agencia o el regulador sectorial notificarán a la Agencia de Protección de Datos Personales sobre la afectación a datos personales derivada del incidente, en los términos de la normativa de protección de datos personales.

7. Sin perjuicio de las disposiciones establecidas en este artículo, el operador de una infraestructura crítica puede notificar al CSIRT sectorial o al CSIRT-CR, según corresponda, sobre cualquier incidente cibernético. Asimismo, cualquier persona u organización, pública o privada, que no sea operador de una infraestructura crítica, podrá notificar a la Agencia sobre cualquier vulnerabilidad o amenaza que haya detectado, o incidente de ciberseguridad del que tenga conocimiento, siempre que lo haga de buena fe conforme al artículo 21.

8. Los CSIRT sectoriales o reguladores sectoriales que reciban un informe sobre un incidente de ciberseguridad significativo, deberán remitir el informe al CSIRT-CR, en los términos señalados vía reglamento. Al recibir dicho informe, el CSIRT-CR lo revisará inmediatamente para determinar si el incidente está relacionado con una amenaza de ciberseguridad o una vulnerabilidad de seguridad en curso y, cuando proceda, utilizará dicho informe para identificar, desarrollar y difundir rápidamente a las partes interesadas, indicadores de ciberamenazas y medidas defensivas anónimas y procesables.

**ARTICULO 21.- Divulgación responsable de vulnerabilidades**

1. No se considerará que una persona, organización o institución pública, infringió disposiciones legales sobre la confidencialidad, integridad y disponibilidad de datos y sistemas de información o que incurrió en un incumplimiento de leyes, reglamentos, contratos y códigos de conducta profesionales, por el hecho de comunicar, publicar o divulgar vulnerabilidades, siempre, que demuestre su buena fe.

2. Con la finalidad de asegurar la buena fe de la persona u organización que divulgue una vulnerabilidad, se deberá tomar en cuenta que no se haya solicitado recompensas bajo coerción o amenaza de publicación de la información; que no se otorgue un tiempo límite para solucionar la vulnerabilidad antes de publicarla o divulgarla; que en el proceso de identificación, la persona u organización tomó las previsiones necesarias para prevenir vulneraciones a la privacidad, degradación o fallas en el servicio y destrucción o manipulación de la data; y que la persona u organización que divulga una vulnerabilidad consideró el impacto de dicha divulgación y tuvo el cuidado razonable para minimizar el daño que pueda causarse por tal divulgación.

3. Del proceso de identificación de vulnerabilidades basadas en la buena fe, quedan excluidos métodos que pudieran conducir a denegación de servicio, a

pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos.

**ARTICULO 22.- Auditorías de Ciberseguridad y Evaluaciones de Riesgo sobre infraestructuras críticas de información**

1. El operador de una infraestructura crítica deberá realizar de forma continua evaluaciones de riesgo cibernético de la infraestructura crítica y presentar reportes de resultados de dichas evaluaciones, al menos una vez al año a la Agencia o el regulador sectorial, según sea el caso.

2. Llevar a cabo auditorías sobre el cumplimiento de esta ley, sus reglamentos y los estándares de ciberseguridad a la Agencia Nacional de Ciberseguridad o el regulador sectorial, al menos una vez cada dos años. Para la realización de estas evaluaciones y auditorias, los operadores, tendrán la facultad de realizar convenios con la Academia, y/o el Colegio Profesional de Informáticos y Computación para estos fines. El operador deberá, a más tardar quince días hábiles después de la finalización de la auditoría o la evaluación del riesgo de ciberseguridad mencionados en el presente artículo, proporcionar el informe de la auditoría o evaluación al regulador sectorial competente, o a la Agencia, según corresponda.

3. Cuando el informe resultante de una auditoría evidencie hallazgos de no conformidad, el regulador sectorial competente o la Agencia, notificará al operador de la infraestructura que lleve a cabo los planes de acción o remediación requeridos para solventar dichos hallazgos, de conformidad con la reglamentación correspondiente. En el caso de los operadores que sean instituciones autónomas o descentralizadas no sujetos a regulación sectorial, o Poderes del Estado, la Agencia remitirá la no conformidad a la auditoría interna de la institución y a la Contraloría General de la República.

**ARTICULO 23.- Suministro de información relacionada con la infraestructura de información crítica**

1. La Agencia como coordinador nacional de ciberseguridad, o el regulador sectorial, según corresponda, podrá solicitar al titular de una infraestructura crítica de información el suministro, dentro de un plazo razonable, lo siguiente:
    a. Información sobre el diseño, la configuración y la seguridad de la infraestructura crítica de información;

    b. Información sobre el diseño, configuración y seguridad de cualquier otro equipo o sistema informático bajo el control del operador que está interconectado, o que se comunica con la infraestructura crítica de información;

    c. Información relativa al funcionamiento de la infraestructura crítica de información, y de cualquier otro equipo o sistema informático bajo el control del operador que esté interconectado con, o que se comunique con la infraestructura crítica de información;

    d. Cualquier otra información que dentro de sus competencias y mediante acto administrativo motivado, se requiera determinar el nivel de ciberseguridad y/o resiliencia de la infraestructura crítica de información.

2. Cuando el operador realice cambios que afecte la ciberseguridad de una infraestructura crítica de información, en relación con el diseño, configuración, seguridad u operación de la infraestructura, después de que se haya proporcionado información de conformidad con el presente artículo, el operador de la infraestructura crítica de información deberá notificar el cambio a la Agencia o el regulador competente, a más tardar treinta días naturales después de la modificación.

**ARTICULO 24.- Cambio en la titularidad o control de la infraestructura de información crítica**

Cuando se produzca algún cambio en la propiedad o control (incluida cualquier participación en dicha propiedad) de una infraestructura crítica de información, el operador deberá informar sobre el mismo, a la Agencia o al regulador sectorial competente, quince días naturales después de la fecha de ese cambio de titularidad o control. El nuevo titular u operador asumirá las mismas obligaciones que el operador anterior, sin necesidad de notificación de la Agencia o del regulador sectorial.

**ARTICULO 25.- Ejercicios de ciberseguridad**

1. La Agencia Nacional de Ciberseguridad o el regulador sectorial competente, según corresponda, coordinará ejercicios de ciberseguridad de manera rutinaria, con el fin de probar el estado de preparación de los operadores de infraestructuras críticas para responder y prevenir incidentes de ciberseguridad.
2. El operador de una infraestructura critica de información, deberá participar en los ejercicios de ciberseguridad que coordinen las autoridades de control.

3. La Agencia adoptará un manual con políticas o procedimientos donde describa el alcance, los tipos de ejercicios, los requerimientos, los indicadores a medir, la frecuencia con la que se realizarán estos ejercicios y esquemas de planificación relacionados.

## Sección Cuarta

## Potestades de investigación y respuesta a incidentes de ciberseguridad significativos

**ARTICULO 26.- Poderes para investigar incidentes de ciberseguridad**

1. Sin perjuicio de la responsabilidad exclusiva del operador de infraestructura crítica de la información de atender, responder, recuperarse e investigar

proactivamente un incidente de ciberseguridad dirigido a su infraestructura crítica, cuando la Agencia o el regulador sectorial hayan recibido una notificación sobre una amenaza o incidente de ciberseguridad, o incluso haya recibido noticias al respecto, dichas autoridades podrán, iniciar la investigación, a efectos de:

a. Evaluar el impacto o el impacto potencial de la amenaza o incidente de ciberseguridad;

b. Prevenir cualquier daño o daño adicional derivado del incidente de ciberseguridad;

c. Evitar que se produzcan nuevos incidentes de ciberseguridad derivados de esa amenaza o incidente de ciberseguridad.

d. Identificar posibles vulnerabilidades de seguridad y valorar eventuales responsabilidades administrativas o judiciales.

2. Para efectos de la investigación citada anteriormente, la autoridad de control tendrá las siguientes facultades:

a. Solicitar, mediante notificación escrita, a las personas relacionadas con los hechos, que evacue o que proporcione una declaración firmada sobre la amenaza o incidente de ciberseguridad;

b. Solicitar la entrega de registros, documentos físicos o electrónicos, o una copia del registro o documento, que no vulneren la confidencialidad y la protección de los datos, aplicando el debido proceso y la normativa vigente, relacionado con los hechos denunciados, proporcione cualquier información relacionada con cualquier asunto relevante para la investigación;

c. Acceder, inspeccionar y comprobar el funcionamiento de un equipo o sistema informático sobre el que se tengan motivos razonables que ha afectado por

el incidente de ciberseguridad, o utilizar dicho equipo o sistema informático para datos, contenidos disponible en dicho equipo o sistema informático; siempre dentro del marco de sus competencias.

d. Indicarle al operador de la infraestructura crítica afectada que tome la/o medidas de colaboración y de apoyo para el desarrollo de la investigación, incluyendo, pero no limitado a:

(i) Preservar el estado del equipo o del sistema informático y/o no utilizarlo;

(ii) Supervisar el equipo o el sistema informático durante un período de tiempo especificado;

(iii) Realizar un análisis forense del equipo o sistema informático para detectar vulnerabilidades de ciberseguridad y evaluar la forma y el grado en que el equipo o el sistema informático afectado por el incidente de ciberseguridad; y

(iv) Permitir que la autoridad de control conecte cualquier equipo al equipo o sistema informático, o instalar en el equipo o sistema informático cualquier programa informático, necesario para el propósito de la investigación.

(v) Escaneo del equipo o sistema informático para detectar vulnerabilidades de ciberseguridad en el equipo o sistema informático;

(vi) Tomar una copia de, o extractos de, cualquier registro electrónico o programa informático contenido en una computadora con respecto a la cual el oficial de respuesta a incidentes tenga conocimiento de afectación por el incidente de ciberseguridad.

## Sección Quinta

## Otras Potestades de las Autoridades de Control sobre las Infraestructuras Críticas de Información

**ARTICULO 27.- Emisión de normas técnicas y directrices**

1. La Agencia Nacional de Ciberseguridad podrá adoptar normas técnicas y directrices generales para el fortalecimiento y gestión unificada de la ciberseguridad de las infraestructuras críticas, en lo siguiente:
   a) El diseño, la configuración, la seguridad y las operaciones de una infraestructura crítica;

   b) Las responsabilidades y deberes de los operadores;

   c) La delimitación de los cambios y tipos de cambios que se considerarán cambios sustanciales de una infraestructura crítica y el procedimiento para su notificación a la Agencia o al regulador sectorial;

   d) La delimitación de los tipos y/o categorías de incidentes de ciberseguridad que pueden presentarse, y de los tipos de incidentes que se considerarán significativos, y el procedimiento para su notificación a la Agencia o al regulador sectorial;

   e) La forma y naturaleza de los ejercicios, pruebas o test de ciberseguridad que se pueden realizar;

   f) El procedimiento para prevenir e investigar los incidentes de ciberseguridad;

   g) Las medidas correctivas que se deben tomar para dar respuesta a las amenazas e incidentes de ciberseguridad.

**ARTICULO 28.- Códigos de práctica y estándares internacionales de seguridad de la información.**

Los reguladores sectoriales podrán adoptar estándares, propios o internacionalmente reconocidos, aplicables a los operadores de su sector, siempre y cuando éstos no ofrezcan una protección menor que la ofrecida por los estándares mínimos que la Agencia declare a cumplir por el sector público y/o los operadores de infraestructuras críticas de información.

**ARTICULO 29.- Potestad de girar instrucciones**

1. La Agencia Nacional de Ciberseguridad o el regulador sectorial, según corresponda, podrá emitir directrices por escrito, ya sea de carácter general o específico, al operador de una infraestructura crítica de información o a una parte de dichos operadores, si considera que:
   a. Para garantizar la ciberseguridad de una infraestructura crítica de información, o una parte de ésta.

   b. Para la administración efectiva de la presente ley.

2. La Agencia podrá revocar en cualquier momento una instrucción emitida en virtud del presente artículo.

3. El operador u operadores afectados por la orden, podrán recurrirla en el plazo y forma establecidos en el reglamento a esta ley.

4. En el caso de operadores de infraestructuras críticas no sometidos a regulación sectorial y que pertenezcan a la Administración Pública Descentralizada o a los Poderes de la República, la Agencia solo podrá emitir alertas en caso de que hayan sufrido un incidente de ciberseguridad, por tratarse de un asunto de seguridad nacional tecnológica, que requiere de la unidad de acción del Estado.

## CAPÍTULO IV

## DE LA CONFIDENCIALIDAD DE INFORMACIÓN EN MATERIA DE CIBERSEGURIDAD

**ARTICULO 30.- Confidencialidad de la información sobre la ciberseguridad de las infraestructuras críticas**

1. Se considera confidencial y reservada la siguiente información:
   a) Las especificaciones técnicas de los sistemas de información, así como los detalles que permitan individualizar su ubicación y forma de suministro eléctrico;

   b) Los datos personales o información comercial sometida al secreto comercial, sustraídos producto de un incidente o de forma no autorizada;

   c) La topología y la arquitectura de la red y de la infraestructura tecnológica y de telecomunicaciones de los operadores de infraestructuras críticas de información;

   d) Los esquemas de direcciones de Protocolo de Internet (IP), públicas y privadas;

   e) Los códigos de acceso, los protocolos de encriptación de los sistemas y redes;

   f) Las rutas de enlace desde las prestadoras de servicios de telecomunicaciones;

   g) Tráfico de Internet entrante y saliente;

   h) Plan de continuidad, y de protección y recuperación ante incidentes;

i) Los datos producidos por las unidades operativas de la Agencia y los CSIRT sectoriales existentes;

j) La que haya sido declarado como tal en virtud de otra Ley;

k) Toda aquella que se declare como tal por parte del Poder Ejecutivo, mediante acto motivado.

2. Los funcionarios o empleados de la Agencia Nacional de Ciberseguridad, de los reguladores sectoriales o CSIRT sectorial, y de los operadores de infraestructuras críticas de información, tienen la obligación de guardar el secreto y confidencialidad que requieren los asuntos relacionados con su trabajo, debido a su naturaleza o en virtud de instrucciones especiales, deber que se mantendrá incluso luego de haber cesado en el cargo.

**ARTICULO 31.- Protección al intercambio de información relevante**

La entrega de información relevante que realicen los operadores de infraestructuras críticas o las instituciones públicas en cumplimiento de esta ley o por requerimiento de las autoridades de control, sea a la Agencia Nacional de Ciberseguridad, a sus unidades operativas, a los reguladores sectoriales competentes, o a los CSIRT sectoriales, y la que éstos se entreguen entre sí, no será considerada como una vulneración de la confidencialidad previamente establecida por leyes, reglamentos, contratos o códigos de conducta profesionales.

Para el intercambio de información de ciberseguridad que involucre datos personales, por regla general, las transferencias deberán realizarse previa anonimización de los datos. En estos casos, el responsable que transferirá los datos deberá cumplir con todas las reglas y disposiciones establecidas en la legislación reguladora de esa materia, incluyendo el deber de realizar la transferencia solo cuando sea estrictamente necesario para los fines perseguidos, cuando ambas

entidades, tanto la que transfiere como la que recibe tengan competencia para tratar esos datos en relación con sus fines y competencias legalmente atribuidas, y siempre que cumplan con el deber de transferir solo los datos estrictamente necesarios para los fines perseguidos. Se prohíben las cesiones masivas e indiscriminadas de bases de datos personales.

## CAPÍTULO V

## GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO

**ARTICULO 32.- Ámbito de aplicación y Competencia de supervisión**

El presente capítulo será aplicable a la totalidad de la Administración Pública, centralizada y descentralizada incluidos los Poderes de la República. Corresponde a la Agencia Nacional de Ciberseguridad la supervisión del cumplimiento de este capítulo, de parte de los órganos y/o instituciones del Poder Ejecutivo, sin perjuicio de las competencias asignadas por la Constitución Política a la Contraloría General de la República. Además, a los reguladores sectoriales la supervisión del cumplimiento de este capítulo, de parte de las instituciones públicas descentralizadas que se encuentren sujetas, en virtud de la ley, a la supervisión de un regulador sectorial, sin perjuicio de las competencias asignadas por la Constitución Política a la Contraloría General de la República.

Corresponde a las auditorías internas y a la Contraloría General de la República, según sea el caso, de conformidad con la Ley Orgánica de la Contraloría General de la República, y la Ley de Control Interno, la supervisión del cumplimiento de este capítulo, de parte de los órganos y/o instituciones de la Administración Pública Descentralizada. Lo anterior, sin perjuicio de las potestades de la Agencia de requerirles la entrega de información necesaria para valorar el estado de seguridad informática de la entidad y de denunciar ante los órganos de control mencionados aparentes irregularidades detectadas, dentro del marco de sus atribuciones. El

incumplimiento de las obligaciones impuestas en este Capítulo se considerará un debilitamiento del sistema de control interno de la entidad, para los efectos de la Ley de Control Interno.

**ARTICULO 33.- Obligaciones generales sobre seguridad de la información**

1. En general, el superior jerárquico de cada institución pública, será responsable de:
   a) Adoptar medidas de seguridad de la información proporcionales al riesgo y la magnitud del daño resultante de un acceso, uso, divulgación, interrupción, modificación, o destrucción no autorizados de la información recogida o mantenida por la entidad o en su nombre; o de los sistemas de información utilizados u operados por la entidad o por un contratista de la entidad, u otra organización en nombre de la entidad;

   b) Velar por el cumplimiento de las normas de seguridad de la información adoptadas por la institución y las políticas y procedimientos emitidos por la Agencia o el regulador sectorial en materia de seguridad de la información.

   c) Garantizar que los procesos de gestión de la seguridad de la información se integren en los procesos de planificación estratégica, operativa, y presupuestaria de la entidad.

   d) Sin perjuicio de lo establecido en la Ley de Control Interno Nº 8292, garantizar que los altos funcionarios proporcionen seguridad de la información para la información y los sistemas de información que apoyan las operaciones y los activos bajo su control, incluyendo:
      i. Evaluación el riesgo y la magnitud del daño que podría resultar del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de dicha información o sistemas de información;
      ii. Determinación de los niveles de seguridad de la información apropiados para proteger dicha información y sistemas de información

de acuerdo con las normas técnicas o estándares promulgados o adoptados por la Agencia.

iii. Aplicación de políticas y procedimientos para reducir los riesgos de forma rentable hasta un nivel aceptable; y

iv. Prueba y evaluación periódica de los controles y técnicas de seguridad de la información para garantizar que se aplican eficazmente;

e) Designar a un Oficial de Seguridad de la Información de la institución, que deberá:

i. Llevar a cabo las responsabilidades del Oficial Jefe de Información bajo esta sección;

ii. Poseer las características profesionales, incluidas en la formación y la experiencia, necesarias para administrar las funciones descritas en esta sección;

iii. Tener funciones de seguridad de la información como tarea principal de dicho funcionario;

iv. Dirigir una oficina con la misión y los recursos necesarios para ayudar a garantizar el cumplimiento de este capítulo de parte de la institución;

v. Desarrollar y mantener un programa de seguridad de la información en toda la agencia, tal como se requiere en el artículo 34;

vi. Formar y supervisar al personal en materia de seguridad de la información con respecto a dichas responsabilidades;

vii. Informar anualmente al superior jerárquico sobre la eficacia del programa de seguridad de la información de la institución, incluyendo el progreso de las acciones correctivas.

f) Garantizar que la institución cuente con personal capacitado suficiente para el cumplimiento de los requisitos de este capítulo y de las políticas, procedimientos, normas y directrices relacionadas;

g) Garantizar que todo el personal sea responsable del cumplimiento del programa de seguridad de la información de toda la institución, implementado según el artículo 34.

**ARTICULO 34.- Plan de Seguridad de la Información**

Cada institución deberá desarrollar, documentar e implementar un programa de seguridad de la información a nivel de toda la institución para proporcionar seguridad a la información y a los sistemas de información que apoyan las operaciones y los activos de la entidad, incluyendo aquellos proporcionados o administrados por otra institución, contratista, proveedor u otra fuente, que incluirá:

a) Evaluaciones periódicas del riesgo y la magnitud del daño que podría resultar del acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción de la información y los sistemas de información que apoyan las operaciones y los activos de la institución;

b) Políticas y procedimientos que se basen en las evaluaciones de riesgo exigidas en el apartado anterior, que reduzcan de forma rentable los riesgos de seguridad de la información a un nivel aceptable y garanticen que la seguridad de la información se aborda a lo largo del ciclo de vida de cada sistema de información de la institución;

c) Formación en materia de seguridad para informar y educar al personal, incluidos los contratistas y otros usuarios de los sistemas de información que apoyan las operaciones y los activos de la entidad, sobre los riesgos de seguridad de la información asociados a sus actividades; y sus responsabilidades en el cumplimiento de las políticas y procedimientos de la agencia diseñados para reducir estos riesgos;

d) Comprobación y evaluación periódicas de la eficacia de las políticas, procedimientos y prácticas de seguridad de la información, que se realizarán

con una frecuencia que dependerá del riesgo, pero no menos de una vez al año.

e) Proceso para planificar, aplicar, evaluar y documentar las medidas correctoras para subsanar cualquier deficiencia en las políticas, procedimientos y prácticas de seguridad de la información de la institución;

f) Procedimientos para detectar, informar y responder a los incidentes de seguridad, que incluyan la forma en que se mitigarán los riesgos asociados a dichos incidentes antes de que se produzcan daños sustanciales, y el deber de notificar y consultar a la Agencia Nacional de Ciberseguridad, en los términos señalados por esta ley o su reglamento.

g) Planes y procedimientos para garantizar la continuidad de las operaciones de los sistemas de información que apoyan las operaciones y los activos de la agencia.

**ARTICULO 35.- Evaluación independiente**

Cada dos años, las instituciones deberán realizar una evaluación del Plan y de las prácticas de seguridad de la información de dicha institución para determinar su eficacia y eficiencia. La evaluación deberá ser efectuada por un tercero independiente, para este fin las instituciones podrán suscribir convenios con la Academia y el Colegio Profesional en informática y Computación, para que puedan realizarlas y que no incurran en gastos, para el cumplimiento de este requisito. La evaluación deberá incluir:

a) Comprobación de la eficacia de las políticas, procedimientos y prácticas de seguridad de la información de un subconjunto representativo de los sistemas de información de la institución; y

b) Evaluación de la eficacia de las políticas, procedimientos y prácticas de seguridad de la información de la agencia;

**ARTICULO 36.- Inventario**

El jerarca de toda institución pública, o el órgano que este designe, elaborará y mantendrán un inventario actualizado de los sistemas de información operados por dicha institución y que se encuentren bajo su control. La identificación de los sistemas de información en un inventario conforme a este artículo incluirá una identificación de las interfaces entre cada uno de dichos sistemas y todos los demás sistemas o redes, incluidos los que no sean operados por la institución o no estén bajo su control. Dicho inventario deberá:

a) Actualizarse cada año en el mes de enero.

b) Estar disponible para la Agencia en los casos en que se requiera, en razón, de seguimiento en cumplimiento de la presente ley, además de la Contraloría General de la República; y

c) Ser un medio de apoyo para la gestión de los recursos de información, incluyendo la planificación, presupuestación, adquisición y gestión de las tecnologías de la información y el seguimiento, las pruebas y la evaluación de los controles de seguridad de la información exigidos en este capítulo.

**ARTICULO 37.- Obligaciones adicionales para reforzar la protección de datos personales sensibles**

En consonancia con las políticas, normas, orientaciones y directrices sobre seguridad de la información en virtud de este capítulo, y los estándares de seguridad de la información aprobados por la Agencia, y el superior jerárquico de cada institución deberá:

a) Identificar, resguardar los datos personales sensibles y de misión crítica almacenados por la institución, de acuerdo con el inventario requerido en el artículo anterior;

b) Evaluar los controles de acceso a los datos descritos en el apartado anterior, la necesidad de un almacenamiento fácilmente accesible de los datos y la necesidad de los individuos de acceder a los datos;

c) Cifrar o hacer indescifrables para los usuarios no autorizados los datos descritos en el apartado a), que se almacenan en los sistemas de información de la institución o que transitan por ellos

## CAPÍTULO VI

## INFRACCIONES Y SANCIONES

**ARTICULO 38.- Potestad sancionatoria**

La potestad sancionatoria respecto de las infracciones administrativas tipificadas en este Capítulo será ejercida:

a) Por el regulador sectorial del sector al que pertenece la infraestructura crítica;

b) En los casos de infraestructuras críticas de sectores que no cuenten con un regulador sectorial, por la Agencia Nacional de Ciberseguridad.

c) En los casos de incumplimientos del capítulo V, por la Agencia Nacional de Ciberseguridad en el caso de incumplimientos del Poder Ejecutivo, y por la Contraloría General de la República en los demás casos, según la Ley Orgánica de dicha entidad y las regulaciones de control interno.

Para establecer la sanción correspondiente, se deberá de respetar los principios del procedimiento administrativo, establecidos en Ley General de Administración Pública.

**ARTICULO 39.- Responsables**

Son responsables por las infracciones administrativas contenidas en esta ley:

1. Los operadores responsables del funcionamiento de una infraestructura crítica de naturaleza privada; y

2. Los operadores responsables del funcionamiento de una infraestructura crítica pertenecientes al Estado.

3. La Administración Pública en el caso de infracciones al capítulo V de esta Ley.

**ARTICULO 40.- Infracciones**

1. Constituyen infracciones los actos y conductas que resulten contrarias a la presente ley. Si se ha incurrido en alguna de las infracciones tipificadas en esta ley, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes:
   a. Para las faltas leves, una multa de uno hasta cinco salarios base.

   b. Para las faltas graves, una multa de seis hasta diez salarios base.

   c. Para las faltas gravísimas, una multa de once hasta quince salarios base.

2. Las sanciones se impondrán, en función de las circunstancias de cada caso individual, se tendrá debidamente en cuenta:
   a. La naturaleza, gravedad y duración de la infracción, teniendo en cuenta el nivel de los daños y perjuicios ocasionados.

b. La intencionalidad o negligencia en la infracción.

c. El carácter continuado de la infracción.

d. Los beneficios obtenidos por el infractor como consecuencia de la comisión de la infracción.

e. La afectación a los derechos de los ciudadanos.

f. Cualquier medida tomada por el responsable para paliar los daños y perjuicios sufridos por los ciudadanos.

g. El grado de responsabilidad de la responsable, habida cuenta de las medidas técnicas u organizativas que hayan aplicado.

h. La reincidencia del infractor.

i. El grado de cooperación con la Agencia o el regulador sectorial con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.

j. La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable notificó la infracción y, en tal caso, en qué medida.

k. Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

l. El riesgo causado de la conducta del infractor para la salud, la seguridad, el ambiente.

3. Si un operador incumpliera de forma intencionada o negligente en una misma actuación, diversas disposiciones de la presente ley, la cuantía total de la sanción no será superior a la cuantía prevista para las infracciones más graves.

Para los efectos de la imposición de multas, se utilizará como unidad de cuenta el concepto de salario base vigente al momento en que se incurra en la falta sancionada, de conformidad con el artículo 2° dispuesto por la Ley N° 7337. El proceso sancionatorio deberá conducirse siguiendo los principios del procedimiento administrativo establecido en la Ley General de la Administración Pública. La imposición y el pago de la multa no eximen al infractor de dejar de atender las disposiciones establecidas por esta ley.

**ARTICULO 41.- Infracciones administrativas leves**

Se considerarán infracciones administrativas leves, las siguientes:

1. Incumplir el deber de notificar cambios significativos que afecten la ciberseguridad de una infraestructura crítica de información, en relación con el diseño, configuración, seguridad u operación de la infraestructura.

2. Incumplir el deber de notificar el cambio de operador o de control sobre una infraestructura crítica;

3. Incumplir el deber de notificar los incidentes de ciberseguridad a las personas afectadas, si fuera el caso;

4. No entregar la información requerida por la Agencia Nacional de Ciberseguridad, los reguladores sectoriales competentes y/o los CSIRT sectoriales dentro del plazo requerido

5. No cumplir con establecer mecanismos técnicos y procedimentales con el fin de detectar amenazas e incidentes de ciberseguridad;

6. No remitir los resultados de la auditoria o la evaluación del riesgo cibernético al Centro Nacional de Ciberseguridad, a los entes u órganos reguladores sectoriales competentes y a los CSIRT sectoriales en los plazos establecidos;

7. No llevar a cabo el inventario previsto en el artículo 36.

8. Incumplir con aquellas obligaciones señaladas en esta ley cuyo incumplimiento negligente o injustificado no tenga señalada una sanción especial.

**ARTICULO 42.- Infracciones administrativas graves.**

Se considerarán infracciones administrativas graves, las siguientes:

1. Reincidir en cualquiera de las infracciones administrativas establecidas como leves;

2. No notificar los incidentes de ciberseguridad a la Agencia Nacional de Ciberseguridad, al regulador sectorial competente y los CSIRT sectoriales, u omitir información que deba contener dicha notificación o reporte, según esta ley;

3. Incumplir con la transferencia prevista en el subinciso a), del inciso 2, del artículo 5 de la presente ley.

4. Omitir llevar a cabo las auditorías o las evaluaciones de riesgo periódicas que exige esta ley.

5. No participar en los ejercicios de ciberseguridad requerido por la Agencia Nacional de Ciberseguridad, los reguladores sectoriales competentes y/o los CSIRT sectoriales; sin causa debidamente justificada.

6. No proporcionar información, registros o documentos requeridos por la Agencia Nacional de Ciberseguridad, los reguladores sectoriales competentes o los CSIRT sectoriales con la finalidad responder a un incidente de ciberseguridad.

7. Incumplir las disposiciones de los reglamentos o normas técnicas generales dictados en materia de ciberseguridad por el regulador sectorial competente o, en su defecto, por la Agencia Nacional de Ciberseguridad.

8. Incumplir alguna o varias de las obligaciones previstas en el artículo 33 o las obligaciones adicionales para reforzar la protección de datos personales sensibles del artículo 37.

**ARTICULO 43.- Infracciones administrativas muy graves**

Se considerarán infracciones administrativas muy graves, las siguientes:

1. Reincidir en cualquiera de las infracciones administrativas establecidas como graves;

2. No implementar un sistema de gestión de riesgo permanente con el fin de identificar aquellos riesgos que pueden afectar la seguridad de los sistemas informáticos, aquellos que afectarían la continuidad operacional del servicio y aquellos que facilitan la ocurrencia de incidentes de ciberseguridad;

3. No responder a los incidentes de ciberseguridad significativos según sus planes y protocolos internos de ciberseguridad, contingencia y continuidad operacional o no adoptar las medidas necesarias para reducir el impacto y la propagación del incidente.

4. Obstruir o impedir que se lleve a cabo una auditoría o evaluación de riesgo;

5. No cumplir con una orden de prohibición de utilizar un sistema de información o cualquiera de sus partes en caso de que la Agencia Nacional de Ciberseguridad, los reguladores sectoriales competentes o los CSIRT sectoriales la hayan notificado;
6. No cumplir con una orden emitida por la Agencia, los reguladores sectoriales competentes o los CSIRT sectoriales con la finalidad de prevenir, detectar o contrarrestar cualquier amenaza o incidente de ciberseguridad significativo;

7. Obstruir las potestades de investigación de la Agencia o el regulador sectorial competente en caso de un incidente de ciberseguridad significativo; y

8. No llevar a cabo el Plan de Seguridad de la Información previsto en el artículo 34 o la evaluación anual independiente del artículo 35.

**ARTICULO 44.- Sanción a funcionarios responsables**

Los funcionarios públicos responsables de la operación de una infraestructura crítica del Estado, o, en función de lo dispuesto del capítulo V de esta ley, los responsables de la institución pública correspondiente, que incurran en algunas de las infracciones administrativas establecidas en los artículos 40, 41 y 42 y se haya demostrado la culpa o dolo en su accionar u omisión, serán sancionados con la suspensión de su cargo por hasta noventa días, sin goce de salario, sin perjuicio de otras sanciones previstas en el régimen disciplinario aplicable al funcionario. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

**ARTICULO 45.- Prescripción de infracciones y sanciones**

Las infracciones administrativas previstas en esta ley prescriben a los tres años contados desde el día en que la infracción se hubiere cometido, o bien, en aquel en que adquiera firmeza la resolución sancionadora.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de doce meses por causas no imputables al presunto infractor.

## CAPÍTULO VII

## COLABORACIÓN CON LAS AUTORIDADES JUDICIALES

**ARTICULO 46.- Colaboración de las entidades de persecución penal con la ciberseguridad.**

Toda autoridad competente que en el curso de una investigación de un delito informático considere que el mismo puede constituir una amenaza de ciberseguridad a una o más infraestructuras criticas nacionales, deberá informar de inmediato a la Agencia Nacional de Ciberseguridad y brindar la colaboración pertinente.

La Agencia Nacional de Ciberseguridad o el regulador sectorial competente deberá informar todo incidente cibernético que pueda constituir un delito informático a las autoridades judiciales competentes.

## CAPITULO VIII

## REFORMAS

**ARTICULO 47.- Reforma a la Ley Nacional de Emergencias y Prevención del Riesgo Nº 8488**

Refórmese el artículo 1 de la Ley Nacional de Emergencias y Prevención del Riesgo Nº 8488 para que en adelante indique lo siguiente:

> “Artículo 1º-**Objeto**. La presente Ley regulará las acciones ordinarias, establecidas en su artículo 14, las cuales el Estado Costarricense deberá

desarrollar para reducir las causas de las pérdidas de vidas y las consecuencias sociales, económicas y ambientales, inducidas por los factores de riesgo de origen natural, antrópico **o tecnológico**; así como la actividad extraordinaria que el Estado deberá efectuar en caso de estado de emergencia, para lo cual se aplicará un régimen de excepción."

**TRANSITORIO I.-** La presente ley entrará en vigor un año después de su publicación, con el propósito de que el Poder Ejecutivo tome las acciones necesarias, durante ese plazo, para instaurar la Agencia que aquí se crea y que los sujetos sometidos a su aplicación puedan adaptarse a las reglas de esta ley.

**TRANSITORIO II.-** El Centro de Inteligencia de Datos en Ciberseguridad (CID-CR), y el El Centro de Intercambio y Monitoreo de Redes (CIMR-CR) aludidos en el artículo 4 de esta ley podrán instaurarse de forma paulatina conforme se vayan generando las condiciones y los recursos técnicos, humanos y económicos necesarios para ello, pero deberán estar instaurados y en funcionamiento en un plazo máximo de dos años a partir de la entrada en vigor de la Ley.

**TRANSITORIO IV.-** El Poder Ejecutivo deberá reglamentar la presente ley dentro de los seis meses posteriores a su entrada en vigencia. Para la promulgación del reglamento deberá procurarse la opinión de los reguladores sectoriales y de los operadores, entidades, empresas e instituciones reguladas, el criterio del Ministerio de Ciencia, Innovación, Tecnología, y Telecomunicaciones, la Superintendencia de Telecomunicaciones, y otros actores relevantes por parte del Poder Ejecutivo. La falta de reglamentación no impedirá la aplicación de esta ley ni su obligatoria observancia, en cuanto sus disposiciones sean suficientes por sí mismas para ello. Rige un año después de su publicación.

**José Joaquín Hernández Rojas y Otros Señores Diputados(as)**

**El expediente legislativo aún no tiene Comisión asignada**