**DECRETO N.° 143**

**LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR,**

**CONSIDERANDO:**

**I.** Que el inciso primero del artículo 1 de la Constitución de la República establece que la persona humana es el origen y el fin de la actividad del Estado, organizando a éste para la consecución de la justicia, de la seguridad jurídica y del bien común.

**II.** Que el uso de las redes y los sistemas de información por parte de los ciudadanos, los organismos y las instituciones del Estado convierte a la digitalización y la conectividad en elementos esenciales en el desarrollo de las actividades de la sociedad y la economía. Asimismo, la información de los individuos, empresas y gobiernos coexiste con estas tecnologías y el ciberespacio; lo cual hace indispensable crear las condiciones para salvaguardar ésta en aras de proteger los intereses públicos y privados en el área de ciberseguridad y seguridad de la información.

**III.** Que en la actualidad existe la amenaza de ciertos comportamientos que tienen el potencial de afectar a la ciudadanía en general, mediante la realización de cualquier acción que tenga como objetivo perjudicar o comprometer la confidencialidad o integridad de la información, la disponibilidad, resiliencia o integridad de sistemas informáticos, equipos, redes, infraestructuras de los órganos del Estado, sus dependencias, las instituciones autónomas, las autoridades municipales o cualquier otra entidad u organismo que administren recursos públicos, bienes del Estado, ejecuten actos de la administración pública en general o posean incidencia en las infraestructuras críticas del país.

**IV.** Que las amenazas antes mencionadas son un riesgo creciente en el ámbito nacional e internacional, convirtiéndolas en una preocupación relevante con respecto al bienestar de la ciudadanía y la continuidad de las actividades gubernamentales; lo cual obliga a que las políticas de la nación generen el marco regulatorio necesario para robustecer y desarrollar la seguridad en dichos ámbitos.

**V.** Que, por lo antes expuesto, se vuelve imprescindible desarrollar el marco regulatorio que permitirá al Estado de El Salvador contar con todas las herramientas necesarias para mantener la continuidad de sus actividades y salvaguardar la seguridad de la información que administra o genera, en aras de garantizar que la ciudadanía conserve los derechos y beneficios que reciben a través de la actividad estatal.

**POR TANTO,**

en uso de sus facultades constitucionales y a iniciativa del presidente de la República, por medio del ministro de Justicia y Seguridad Pública,

**DECRETA la siguiente:**

## LEY DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

### CAPÍTULO I
### DISPOSICIONES GENERALES

**Objeto**

**Art. 1.-** La presente ley tiene como objeto establecer los principios, el marco legal, la institucionalidad, los lineamientos, así como las políticas de protección que permitan estructurar, regular, auditar y fiscalizar las medidas de ciberseguridad y seguridad de la información en poder de las instituciones públicas.

**Ámbito de aplicación**

**Art. 2.-** Están obligados al cumplimiento de esta ley los órganos del Gobierno, sus dependencias, las instituciones oficiales autónomas, las autoridades municipales o cualquier otra entidad u organismo, independientemente de su forma, naturaleza o situación jurídica, mediante las cuales se administren recursos públicos, bienes del Estado, ejecuten actos de la administración pública en general o que posean incidencia en las infraestructuras críticas de la nación.

Se incluyen dentro de los recursos públicos aquellos fondos provenientes de Convenios o Tratados que celebre el Estado de El Salvador con otros Estados o con Organismos Internacionales, a menos que el Convenio o Tratado determine requisitos superiores en materia de ciberseguridad o seguridad de la información.

En consecuencia, todos los servidores públicos, dentro o fuera del territorio de la República, y las personas que laboren en las entidades mencionadas en este artículo, están obligados al cumplimiento íntegro de la presente ley.

**Principios rectores**

**Art. 3.-** La presente ley contempla los siguientes principios:

a) **Seguridad por diseño:** los sujetos establecidos dentro del ámbito de aplicación de la presente ley deberán aplicar un enfoque de seguridad por diseño en el desarrollo, compra, aprovisionamiento, implementación y gestión de sistemas informáticos o equipos tecnológicos y en los procesos de administración de éstos, de manera que la ciberseguridad y seguridad de la información sea el objetivo originario, transversal y permanente durante la operación o utilización de los mismos.

b) **Resiliencia, continuidad y disponibilidad:** las medidas o acciones que se adopten en atención a la presente ley deben tener como propósito la reducción de los efectos adversos de los incidentes de ciberseguridad o seguridad de la información, la recuperación en el menor plazo posible y la continuidad y el fomento de la resistencia de las actividades críticas que dependen de los sistemas de información comprometidos.

c) **Gestión de riesgos:** evaluar y gestionar continuamente los riesgos de ciberseguridad o seguridad de la información, identificando las amenazas potenciales y aplicando medidas de mitigación adecuadas.

d) **Cooperación:** consiste en el deber de apoyar recíprocamente con la autoridad competente a fin de prevenir, detectar y responder a las amenazas o incidentes de ciberseguridad o seguridad de la información. Tal cooperación podrá materializarse mediante la interconexión, interdependencia de los sistemas informáticos u otras medidas adecuadas para ese fin.

e) **Control de daños:** las medidas o actuaciones frente a amenazas o incidentes de ciberseguridad o seguridad de la información deberán ser adoptadas y realizarse de forma oportuna y diligente, en aras de evitar el incremento de los daños y las vulneraciones a los sistemas, información y servicios, así como la posible afectación de otras áreas u operaciones.

f) **Seguridad en el ciberespacio y sus anexos:** los sujetos obligados por la presente ley deberán realizar todas las medidas posibles y necesarias para resguardar la seguridad de las redes, equipos y sistemas informáticos que se utilicen para el ejercicio de sus actividades y funciones, así como aquellas en las que almacenen, procesen y administren su información o la de sus usuarios.

g) **Racionalidad, responsabilidad y proporcionalidad:** las medidas o acciones que se implementen frente a las amenazas o incidentes de ciberseguridad o seguridad de la información deberán aplicarse de forma ecuánime, equitativa y adecuada al nivel de exposición a los riesgos inherentes a éstas, los daños que produzcan o su eventual impacto social y económico.

h) **Confidencialidad:** implementar las medidas, acciones o herramientas necesarias para garantizar que los sistemas informáticos, redes o información solo sean accesibles a los empleados, funcionarios, autoridades o usuarios autorizados para ello, protegiendo así la privacidad de los ciudadanos.

i) **Integridad:** acreditar la confiabilidad y exactitud de la información que gestionen o administren los sujetos obligados por la presente ley, evitando cualquier modificación a través del tiempo, alteración, corrupción o eliminación no autorizada.

j) **Neutralidad tecnológica:** la cual sustenta la no discriminación entre tecnologías, en la medida que ellas consistan en medios seguros y eficientes a través de los cuales sea posible dar cumplimiento a lo establecido en la presente ley.

**Definiciones**

**Art. 4.-** Para los efectos de la presente ley se entenderá por:

a) **Amenaza:** toda acción, comportamiento o evento, real o potencial, que permita el ataque, invasión, vulneración o inhabilitación sobre los sistemas informáticos, equipos, redes o infraestructuras de los sujetos obligados por la presente ley.

b) **Evento:** hecho observable derivado de un acontecimiento en un sistema informático, equipo, red o infraestructura, que en caso de materializarse cambiaría un conjunto particular de circunstancias de los mismos.

c) **Incidente:** toda acción, comportamiento o evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad, resiliencia o integridad de sistemas informáticos, equipos, redes, infraestructuras o procesos ejecutados o implementados en éstos.

d) **Infraestructuras críticas:** sistemas informáticos, equipos, redes o infraestructuras o servicios tecnológicos que soportan o asisten en la prestación de los servicios esenciales

para la ciudadanía y que en ocasión de fallo podrían tener un impacto en éstos.

e) **Ciberespacio:** ambiente digital que no tiene límites físicos y/o geográficos y permite la interconexión o comunicación entre sistemas informáticos, equipos o infraestructuras.

f) **Riesgo cibernético o informático:** medida de la probabilidad de ocurrencia y potenciales resultados negativos, derivados de una falla o vulneración a las medidas de seguridad informática o de la información, que pueden afectar la privacidad, la integridad o la disponibilidad de los datos y/o servicios que se encuentran resguardados en el sistema informático.

g) **Servicio esencial:** es todo servicio que sea necesario para la seguridad nacional, defensa de la soberanía, economía del país, relaciones exteriores, mantenimiento del orden público, salud, bienestar de la ciudadanía y la realización de actividades sociales cruciales.

h) **Sistema Informático:** es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información.

i) **Vulnerabilidad:** cualquier debilidad de un sistema informático, equipo, red o infraestructura o en las medidas o políticas de seguridad que les apliquen a éstas, que pudiera derivar en una amenaza o incidente.

j) **Activo de información:** cualquier elemento valioso para los sujetos obligados por la presente ley y que tienen incidencia en los procesos o funciones que realizan.

k) **Autenticación:** propiedad de la información que da cuenta de su origen legítimo.

l) **Infraestructura de telecomunicaciones:** conjunto de técnicas, equipamiento, sistemas y procesos que permiten la transmisión a distancia de información, ya sea en forma de voz, datos, texto, imágenes o cualquier otra forma entre usuarios.

**Del riesgo informático**

**Art. 5.-** Para efectos de la presente ley, se entenderá que existe riesgo informático cuando los sujetos regulados en el artículo 2 incumplan las normativas, protocolos, lineamientos, estándares y criterios técnicos establecidos por la Agencia de Ciberseguridad del Estado, los cuales se basarán en estándares nacionales o internacionales en materia de ciberseguridad y seguridad de la información.

Las disposiciones referidas en el inciso anterior deberán tener como marco de referencia los requerimientos técnicos o estándares emitidos por organizaciones que cuente con el reconocimiento de la industria en la que se pretenden aplicar, por sus aportes a la estandarización del rubro en cuestión, o que cuenten con experiencia probada a nivel internacional, siempre que esté demostrada la funcionalidad, eficiencia y beneficio de dichos requerimientos o estándares en materia de ciberseguridad y seguridad de la información.

**Obligaciones**

**Art. 6.-** Los sujetos a quienes aplique la presente ley de conformidad con el Art. 2, tendrán las obligaciones siguientes:

a) Implementar un sistema de gestión de ciberseguridad y seguridad de la información permanente con el fin de determinar y mitigar aquellos riesgos que puedan afectar la seguridad de los sistemas e infraestructuras informáticas, abarcando equipos, redes, infraestructuras de telecomunicaciones o procesos ejecutados o implementados en éstos.

b) Elaborar una estrategia de seguridad informática y de la información apegado a estándares o marcos de referencia nacionales e internacionales.

c) Mantener un registro actualizado de todas las acciones ejecutadas que compongan el sistema de gestión de ciberseguridad y seguridad de la información.

d) Elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán ser aprobados por la autoridad competente y se someterán a revisiones periódicas de conformidad con los lineamientos aplicables.

e) Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las medidas, sistemas informáticos, equipos, redes, infraestructuras o procesos ejecutados o implementados en éstos; todo, en aras de detectar elementos o riesgos que comprometan la ciberseguridad y la seguridad de la información.

f) Aplicar y cumplir de manera inmediata y eficaz las medidas necesarias para prevenir, reportar y resolver las amenazas de ciberseguridad y seguridad de la información, de conformidad con las disposiciones jurídicas establecidas al respecto.

g) Adoptar de forma oportuna, expedita y eficiente las acciones necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o seguridad de la información.

h) Remitir en el tiempo, forma y especificidad los informes relacionados con la ciberseguridad y seguridad de la información que le sean exigidos por la autoridad competente.

i) Crear o designar un área o áreas responsables para la implementación, seguimiento, revisión y adecuación de las acciones y medidas relacionadas con la ciberseguridad y seguridad de la información pertinentes, otorgándoles internamente independencia y atribuciones necesarias para ejecutar sus funciones sin obstáculos o trámites previos, pero en estrecha coordinación con la autoridad competente en materia de ciberseguridad y seguridad de la información.

j) Cumplir con los requerimientos de información o instrucciones que realice la autoridad competente, en el tiempo, forma y especificidades correspondientes.

k) Facilitar las labores de gestión, auditoría e inspección que realice la autoridad competente en materia de ciberseguridad y seguridad de la información.

l) Informar a los potenciales afectados, en la medida que puedan identificarse y cuando así

lo determine la Agencia de Ciberseguridad del Estado, sobre la ocurrencia de incidentes que pudieran comprometer o comprometan gravemente su información, así como las posibles medidas que pueden adoptar para mitigar los riesgos ocasionados por los mismos, si las hubiere. Esta obligación de informar deberá cumplirse a través de los medios o mecanismos que determine la referida autoridad.

m) Realizar las planificaciones, gestiones y trámites necesarios para implementar las obligaciones que deriven de la presente ley, así como de las disposiciones que se emitan en atención a esta, de manera oportuna.

n) Las demás que establecieran las disposiciones contenidas en políticas, normativas, protocolos, lineamientos, estándares y criterios técnicos en materia de ciberseguridad y seguridad de la información.

La autoridad competente emitirá las disposiciones pertinentes en materia de ciberseguridad y seguridad de la información de conformidad a lo establecido en la letra b) del artículo 8 de la presente ley, con la finalidad que, los sujetos obligados por la presente ley se mantengan en estricta coordinación con la misma y cumplan con las obligaciones establecidas en este artículo.

## CAPÍTULO II
## AGENCIA DE CIBERSEGURIDAD DEL ESTADO

### Creación de la Agencia

**Art. 7.-** Créase la Agencia de Ciberseguridad del Estado, que en lo sucesivo se denominará "ACE" o la "Agencia", como una dependencia del Estado, de Derecho Público, con carácter técnico, con personalidad jurídica y patrimonio propio, de duración indefinida, con autonomía administrativa y financiera.

La ACE tendrá su domicilio en la capital de la República y estará facultada para establecer oficinas en cualquier lugar del territorio nacional.

### Atribuciones

**Art. 8.-** La Agencia tendrá las atribuciones siguientes:

a) Elaborar la Política de Ciberseguridad y Seguridad de la Información de la Nación, misma que contendrá los lineamientos, planes y programas de acción que se aplicarán para su cumplimiento, y someterla a aprobación del presidente de la República.

b) Emitir las normativas, protocolos, lineamientos, estándares y criterios técnicos, tanto generales como específicas, basadas en las mejores prácticas y marcos de referencia internacionales en materia de ciberseguridad y seguridad de la información; de acuerdo con lo establecido en el artículo 5 y en concordancia con la Política de Ciberseguridad y Seguridad de la Información de la Nación.

c) Crear e implementar los programas de acción necesarios para responder ante las amenazas o incidentes de ciberseguridad y seguridad de la información que involucren a los sujetos obligados por la presente ley.

d) Requerir a las entidades obligadas por la presente ley que se hayan visto afectados sus

sistemas informáticos, equipos, redes o infraestructuras por un incidente de ciberseguridad o seguridad de la información, las acciones que sean necesarias para el cumplimiento de sus fines.

e) Crear y administrar un Registro Nacional de Amenazas e Incidentes de Ciberseguridad.

f) Calificar, mediante resolución fundada, a los operadores de infraestructuras críticas, y someterlo a ratificación del presidente de la República.

g) Retirar la calificación, mediante resolución fundada, a los operadores de infraestructuras críticas, y someterlo a ratificación del presidente de la República.

h) Requerir a las entidades obligadas por la presente ley que hayan sufrido un incidente de ciberseguridad o seguridad de la información, que entreguen a los potenciales afectados o autoridades de investigación información veraz, suficiente y oportuna sobre dicha circunstancia, conforme lo dispuesto en el literal l) del artículo 6.

i) Diseñar e implementar planes y campañas de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad y seguridad de la información.

j) Requerir, a los sujetos obligados por la presente ley, el acceso a la información necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o seguridad de la información y gestionar amenazas o incidentes que ya hubieren ocurrido. Cuando la información referida incluya datos personales, éstos deberán ser tratados con el propósito de anonimizar a sus titulares, siempre que ello sea posible, sin entorpecer la gestión de incidentes.

k) Establecer los mecanismos de coordinación y colaboración entre el área o áreas responsables para la implementación, seguimiento, revisión y adecuación de las acciones y medidas relacionadas con la ciberseguridad y seguridad de la información que establezcan los sujetos obligados por la presente ley.

l) Establecer los requisitos técnicos y la forma de llevar a cabo las auditorías y evaluaciones de riesgo sobre ciberseguridad y seguridad de la información que debe realizar para garantizar el cumplimiento de la presente ley y demás disposiciones que se emitan sobre dicho ámbito.

m) Efectuar revisiones de las medidas y acciones de ciberseguridad y seguridad de la información implementadas por los sujetos obligados por la presente ley, a fin de establecer mecanismos de mejora y prevención de riesgos, asegurando la utilización de medidas o herramientas adecuadas y actualizadas, para responder a las amenazas derivadas del uso de nuevas tecnologías.

n) Fomentar la cooperación con organismos internacionales y autoridades extranjeras en temas relacionados con la ciberseguridad y seguridad de la información.

o) Representar al país ante Organismos Internacionales relacionados con las políticas de ciberseguridad y seguridad de la información.

p) Imponer sanciones conforme a la presente ley.

q) Dictar, modificar o anular medidas provisionales según lo dispuesto en la Ley de Procedimientos Administrativos.

r) Estudiar y someter a consideración del Órgano Ejecutivo a través del Ramo de Justicia y Seguridad Pública, propuestas de ley o reformas a disposiciones vigentes en materia de ciberseguridad y seguridad de la información.

s) Aprobar el reglamento interno, así como los manuales y otros instrumentos necesarios para la administración de la Agencia.

t) Proponer los proyectos de presupuesto especial y sistema de salarios de la ACE y remitirlos al Ministerio de Hacienda para su respectiva aprobación en la Asamblea Legislativa.

u) Auxiliar a la Fiscalía General de la República, Órgano Judicial y a otras instituciones públicas que le requieran, en actividades de pericia forense relacionadas con las funciones que realiza.

v) Dar aviso a la Fiscalía General de la República en un plazo máximo de setenta y dos horas, cuando en el ejercicio de sus facultades o con ocasión de ellas, advierta que existen elementos que pudieren configurar algún delito de los contemplados en la Ley Especial contra los Delitos Informáticos y Conexos u otras leyes penales.

w) Definir y coordinar la implementación de programas de capacitación y concienciación relacionados con la materia de ciberseguridad y seguridad de la información; para lo cual podrá apoyarse de otras instituciones públicas o entidades privadas u organismos nacionales o internacionales.

x) Ejercer las demás atribuciones o facultades que legalmente le correspondan o necesarias para el cumplimiento de la presente ley u otras que le apliquen.

**Representación legal y organización administrativa**

**Art. 9.-** La ACE tendrá, como mínimo, la siguiente organización administrativa: un Director General, un Director de Ciberseguridad y Seguridad de la Información y las dependencias o unidades administrativas que establezca su reglamento interno, según las necesidades para garantizar la aplicación de la presente ley y la disponibilidad de recursos del Estado.

El Director General será la máxima autoridad y el representante legal de la Agencia, y ejercerá las atribuciones y facultades que correspondan a la ACE, a excepción de la potestad para imponer sanciones. Dicho funcionario será nombrado por el presidente de la República, y fungirá por un periodo de tres años prorrogables.

De la misma forma será nombrado el Director de Ciberseguridad y Seguridad de la Información, quien asistirá al Director General en el ejercicio de sus atribuciones y facultades, en cumplimiento de la presente ley.

El Director de Ciberseguridad y Seguridad de la Información conocerá de los procedimientos administrativos para imponer las sanciones que establece la presente ley, y podrá delegar la instrucción y sustanciación de estos procedimientos, no así la imposición de la sanción, en un

empleado o funcionario de la ACE distinto del Director General.

La Agencia establecerá las dependencias o unidades administrativas de su estructura y el funcionamiento de éstas en un reglamento interno.

**Requisitos**

**Art. 10.-** Para ser Director General de la ACE se requiere:

a) Ser mayor de treinta y cinco años de edad.

b) Tener un grado universitario, nacional o extranjero, de preferencia en informática, ciencias de la computación, ingeniería en sistemas, telecomunicaciones u otras áreas relacionadas.

c) Acreditar experiencia profesional y laboral en materia de ciberseguridad o seguridad de la información.

d) Ser de reconocida honorabilidad y probidad.

e) Haberse desempeñado en forma destacada en asuntos profesionales, de servicio público o académico.

El Director de Ciberseguridad y Seguridad de la Información deberá cumplir con los requisitos establecidos en el presente artículo, con excepción de lo establecido en el literal a).

**Impedimentos e incompatibilidades**

**Art. 11.-** No podrán ser nombrados en el cargo de director general o director de Ciberseguridad y Seguridad de la Información, las personas siguientes:

a) El cónyuge o parientes dentro del cuarto grado de consanguinidad o segundo de afinidad del presidente o vicepresidente de la República.

b) El cónyuge o parientes dentro del cuarto grado de consanguinidad o segundo de afinidad de los ministros o viceministros de Estado.

c) El cónyuge o parientes dentro del cuarto grado de consanguinidad o segundo de afinidad de cualquiera de los titulares o miembros de los órganos de dirección de los sujetos obligados por la presente ley.

d) Los que desempeñen cargos en los órganos de dirección de partidos políticos, asociaciones empresariales, sindicales o de consumidores.

e) Los directores o administradores de sociedades mercantiles.

El desempeño de ambos cargos será de dedicación exclusiva y es incompatible con el ejercicio de cualquier cargo público, actividad profesional o mercantil, tanto nacional como internacional, a excepción de la docencia universitaria, siempre y cuando ésta no vaya en menoscabo del desarrollo de sus funciones.

**Cesación del cargo**

**Art. 12.-** El Director General o Director de Ciberseguridad y Seguridad de la Información cesarán en el ejercicio del cargo por renuncia o remoción que haga el Presidente de la República, cuando:

a) Se compruebe incumplimiento grave de sus obligaciones.

b) Se compruebe omisión dolosa de sus obligaciones.

c) Incapacidad sobreviniente física o mental que imposibilite el ejercicio de las mismas.

d) Condena firme por delito doloso.

e) Por conducta privada o profesional notoriamente inmoral.

f) Por prevalerse del cargo para ejercer influencias indebidas.

**Sustitución temporal**

**Art. 13.-** En los casos de incapacidad física o mental de carácter temporal, renuncia o destitución del Director General, el Director de Ciberseguridad y Seguridad de la Información sustituirá al mismo hasta que el Presidente de la República nombre a otra persona para el ejercicio del cargo.

**Presupuesto**

**Art. 14.-** La ACE tendrá un presupuesto especial y su propio sistema de salarios. Los proyectos respectivos serán preparados de conformidad con lo establecido en la ley Orgánica de Administración Financiera del Estado y serán sometidos a aprobación de la Asamblea Legislativa.

**Patrimonio**

**Art. 15.-** El patrimonio de la Agencia estará constituido por:

a) Los recursos que el Estado le confiera inicialmente.

b) Las asignaciones que anualmente se establezcan con cargo a su presupuesto especial.

c) Los recursos que reciba en virtud de programas de asistencia de gobiernos u organismos nacionales e internacionales.

d) Los bienes muebles e inmuebles, valores o derechos que adquiera a cualquier título.

La ACE estará sujeta a la fiscalización de la Corte de Cuentas de la República; adicionalmente deberá contratar anualmente los servicios de una firma especializada para que realice auditoría externa de sus actuaciones.

**Confidencialidad**

**Art. 16.-** Los funcionarios y empleados de la Agencia tendrán la obligación de guardar el

secreto y estricta confidencialidad de la información que tuvieren acceso en virtud de las funciones y actividades laborales que realicen, esta obligación se mantendrá aún después de haber cesado en el cargo por un periodo mínimo de cinco años.

Se prohíbe a las autoridades, funcionarios, empleados, delegados, peritos, agentes o personas que presten servicios a la Agencia, a cualquier título, ya sea de carácter temporal o permanente, revelar cualquier información que hayan obtenido en el desempeño de su cargo o aprovecharse de tal información para fines personales o de terceros.

En el caso de los servidores públicos que presten sus servicios a la Agencia, el incumplimiento de lo establecido en el presente artículo constituirá causal de despido o destitución sin responsabilidad para la referida autoridad, sin perjuicio de la responsabilidad civil, penal o de cualquier otra naturaleza a que hubiere lugar.

## CAPÍTULO III
## INFRACCIONES, SANCIONES, PROCEDIMIENTOS Y RECURSOS

### Principios de legalidad, culpabilidad y proporcionalidad

**Art. 17.-** Las infracciones a las disposiciones de la presente ley serán sancionadas administrativamente, en los casos y en la forma regulada en los artículos de este título, sin perjuicio de las responsabilidades civiles, penales o de otro orden en que puedan incurrir.

Los sujetos obligados por la presente ley serán responsables por las infracciones administrativas establecidas en este capítulo, por acción u omisión, a título de dolo, culpa o cualquier otro título que determine el ordenamiento jurídico.

A las infracciones y sanciones que se impongan en virtud de la presente ley le serán aplicables los principios de la potestad sancionadora previstos en la Ley de Procedimientos Administrativos; especialmente el de proporcionalidad, en virtud del cual será necesario guardar la debida adecuación entre la gravedad del hecho constitutivo de infracción y la sanción aplicada.

### Clasificación de las infracciones

**Art. 18.-** Las infracciones a las que se refiere esta ley se clasifican en: leves, graves o muy graves.

### Infracciones leves

**Art. 19.-** Se considerarán infracciones leves las siguientes:

a) Remitir, fuera del plazo, los informes o la información relacionados con la ciberseguridad y seguridad de la información que le sean exigidos por la Agencia, siempre y cuando tal información no se relacione con algún incidente o sea necesaria para la gestión de éste.

b) Presentar, sin las especificaciones requeridas, los informes o la información relacionados con la ciberseguridad y seguridad de la información que le sean exigidos por la ACE, siempre y cuando tal información no se relacione con algún incidente o sea necesaria para la gestión de éste.

c) Incumplir las disposiciones contenidas en las políticas, normativas técnicas, lineamientos

e instructivos en materia de ciberseguridad y seguridad de la información, cuando éstas no tengan incidencia en la implementación del sistema de gestión de ciberseguridad y seguridad de la información o la gestión de incidentes.

También incurrirán en responsabilidad los titulares, la alta dirección y cualquier otro funcionario o empleado por las infracciones anteriores cuando éstas se materialicen en virtud de la orden, instrucción, negligencia u omisión de éstos.

**Infracciones graves**

**Art. 20.-** Se considerarán infracciones graves las siguientes:

a) No contar con un registro actualizado de todas las acciones ejecutadas que compongan el sistema de gestión de ciberseguridad y seguridad de la información.

b) No elaborar y remitir, en tiempo y forma, los planes de continuidad operacional y ciberseguridad para la aprobación de la Agencia.

c) No implementar los planes de continuidad operacional y ciberseguridad aprobados por la ACE.

d) No realizar continuamente las operaciones de revisión, ejercicios, simulacros y análisis de las medidas, sistemas informáticos, equipos, redes, infraestructuras o procesos ejecutados o implementados en éstos.

e) Incumplir las disposiciones contenidas en las políticas, normativas técnicas, lineamientos e instructivos en materia de ciberseguridad y seguridad de la información, cuando éstas se relacionen con la implementación del sistema de gestión de ciberseguridad y seguridad de la información o la gestión de incidentes.

f) Obstaculizar o impedir las labores del área o áreas responsables para la implementación, seguimiento, revisión y adecuación de las acciones y medidas relacionadas con la ciberseguridad y seguridad de la información.

g) Presentar a la ACE información incompleta, errónea o inexacta.

También incurrirán en responsabilidad los titulares, la alta dirección y cualquier otro funcionario o empleado por las infracciones anteriores cuando éstas se materialicen en virtud de la orden, instrucción, negligencia u omisión de éstos.

**Infracciones muy graves**

**Art. 21.-** Se considerarán infracciones muy graves las siguientes:

a) Remitir, fuera del plazo, los informes o la información relacionados con la ciberseguridad y seguridad de la información que le sean exigidos por la autoridad competente, cuando tal información se relacione con algún incidente o sea necesaria para la gestión de éste.

b) Presentar, sin las especificaciones requeridas, los informes o la información relacionados con la ciberseguridad y seguridad de la información que le sean exigidos por la autoridad competente, cuando tal información se relacione con algún incidente o sea necesaria

para la gestión de éste.

c) No implementar un sistema de gestión de ciberseguridad y seguridad de la información permanente, sin causa justificada, de acuerdo con lo establecido por la Agencia.

d) Incumplir con las medidas necesarias para prevenir, reportar y resolver las amenazas de ciberseguridad y seguridad de la información, de manera inmediata y eficaz.

e) No adoptar, de forma oportuna, expedita y eficiente, las acciones necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o seguridad de la información.

f) No crear o designar un área o áreas responsables para la implementación, seguimiento, revisión y adecuación de las acciones y medidas relacionadas con la ciberseguridad y seguridad de la información.

g) Obstaculizar o impedir las labores de gestión, auditoria e inspección que realice la Agencia en materia de ciberseguridad y seguridad de la información.

h) No informar a los potenciales afectados, en la medida que puedan identificarse y cuando así lo determine la ACE, sobre la ocurrencia de incidentes que pudieran comprometer o comprometan gravemente su información, así como las posibles medidas que pueden adoptar para mitigar los riesgos ocasionados por los mismos, si las hubiere.

i) Incumplir con las órdenes de prohibición de utilizar los sistemas informáticos o cualquiera de sus partes, en el tiempo y la forma en que sea comunicada por la Agencia.

También incurrirán en responsabilidad los titulares, la alta dirección y cualquier otro funcionario o empleado por las infracciones anteriores cuando éstas se materialicen en virtud de la orden, instrucción, negligencia u omisión de éstos.

**Sanción para infracciones leves**

**Art. 22.-** Las infracciones leves se sancionarán con amonestación escrita o una multa de entre uno a diez salarios mínimos mensuales del sector comercio, según corresponda al sujeto obligado.

El funcionario o empleado que reciba tres o más amonestaciones escritas en un plazo menor a un año será desvinculado de su empleo o cargo sin responsabilidad para la Administración Pública.

**Sanción para infracciones graves**

**Art. 23.-** Las infracciones graves se sancionarán con despido o destitución del cargo sin responsabilidad para la Administración Pública y una multa de entre once a cincuenta salarios mínimos mensuales del sector comercio cuando el infractor se encuentre vinculado con el sector público.

En el caso de que el infractor sea del sector privado, la sanción será una multa de entre once a cincuenta salarios mínimos mensuales del sector comercio.

**Sanción para infracciones muy graves**

**Art. 24.-** Las infracciones graves se sancionarán con despido o destitución del cargo sin responsabilidad para la Administración Pública y una multa de entre cincuenta y un a cien salarios mínimos mensuales del sector comercio cuando el infractor se encuentre vinculado con el sector público.

En el caso de que el infractor sea del sector privado, la sanción será una multa de entre cincuenta y un a cien salarios mínimos mensuales del sector comercio.

**Imposibilidad de pertenecer al sector público**

**Art. 25.-** El funcionario o empleado que sea despedido o destituido de su cargo por la comisión de algunas de las infracciones contempladas por la presente ley, no podrá laborar para la administración pública por un periodo de diez años posteriores a la imposición de la sanción respectiva.

**Medidas adicionales**

**Art. 26.-** Determinada la procedencia de la sanción, la Agencia podrá ordenar al infractor o el sujeto obligado relacionado que adopte las medidas que fueren necesarias para restablecer la legalidad alterada por la infracción o que permita la corrección de los derechos o las situaciones vulneradas.

Todas las sanciones determinadas en la presente ley no eximen al infractor de las responsabilidades civiles o penales derivadas de las investigaciones correspondientes a que dieren lugar.

**Multa coercitiva**

**Art. 27.-** Con el fin de lograr la ejecución de sus actos, la Agencia podrá imponer multas coercitivas de entre uno a diez salarios mínimos del sector comercio por cada día hábil que transcurra sin que se cumpla con lo ordenado.

Esta sanción será independiente y compatible con las demás sanciones que contempla esta ley.

**Procedimiento sancionador**

**Art. 28.-** El procedimiento para la determinación de las infracciones y sanciones que establece la presente ley deberá realizarse de conformidad con el procedimiento simplificado contemplado en la Ley de Procedimientos Administrativos.

El procedimiento podrá iniciarse de oficio, por aviso, por denuncia o por cualquier otro medio. Cuando la información sobre la presunta comisión de la infracción se recibiera de forma verbal o de tal manera que no hubiera un respaldo escrito de la misma, la Agencia levantará un acta con todos los datos pertinentes para la tramitación del procedimiento.

**Prescripción**

**Art. 29.-** Las infracciones y sanciones contempladas en la presente ley prescribirán a los

cinco años.

## CAPÍTULO IV
## DISPOSICIONES FINALES

**Especialidad y supletoriedad**

**Art. 30.-** La presente ley, por su carácter especial, prevalecerá sobre toda otra disposición legal que la contraríe, incluyendo aquellas que regulen la relación laboral entre empleados, servidores y funcionarios públicos; sin embargo, siempre deberán respetarse las garantías constitucionales de estos mismos. En todo lo no previsto, se aplicará supletoriamente lo dispuesto en la Ley de Procedimientos Administrativos.

**Emisión de normativas y disposiciones aplicables**

**Art. 31.-** La ACE deberá elaborar las normativas, protocolos, lineamientos, estándares y criterios técnicos, tanto generales como específicos, en materia de ciberseguridad y seguridad de la información, en concordancia con lo establecido en el artículo 5, a más tardar noventa días contados a partir de la vigencia de la presente ley.

**Vigencia**

**Art. 32.-** La presente ley entrará en vigencia ocho días después de su publicación en el Diario Oficial.

DADO EN EL SALÓN AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los doce días del mes de noviembre del año dos mil veinticuatro.

ERNESTO ALFREDO CASTRO ALDANA,
PRESIDENTE.

SUECY BEVERLEY CALLEJAS ESTRADA,
PRIMERA VICEPRESIDENTA.

KATHERYN ALEXIA RIVAS GONZÁLEZ,
SEGUNDA VICEPRESIDENTA.

ELISA MARCELA ROSALES RAMÍREZ,
PRIMERA SECRETARIA.

REYNALDO ANTONIO LÓPEZ CARDOZA,
SEGUNDO SECRETARIO.

REINALDO ALCIDES CARBALLO CARBALLO,
TERCER SECRETARIO.

CASA PRESIDENCIAL: San Salvador, a los catorce días del mes de noviembre de dos mil veinticuatro.

PUBLÍQUESE,

NAYIB ARMANDO BUKELE ORTEZ,
Presidente de la República.

HÉCTOR GUSTAVO VILLATORO,
Ministro de Justicia y Seguridad Pública.

D. O. N° 219
Tomo N° 445
Fecha: 15 de noviembre de 2024

JE/gm
29-11-2024