Año: 2025 **Expediente: 20258/LXXVII**

H. Congreso del Estado de Nuevo León

LXXVII Legislatura

PROMOVENTE: LOS CC. DIP. MARIO ALEJANDRO SOTO ESQUER, COORDINADOR DEL GRUPO LEGISLATIVO DE MORENA, DIP. MARÍA GUADALUPE RODRÍGUEZ MARTÍNEZ, COORDINADORA DEL GRUPO LEGISLATIVO DEL PARTIDO DEL TRABAJO, DIP, CLAUDIA MAYELA CHAPA MARMOLEJO, COORDINADORA DEL GRUPO LEGISLATIVO DEL PARTIDO VERDE ECOLOGISTA DE MÉXICO Y LOS INTEGRANTES DEL GRUPO LEGISLATIVO DE MORENA DE LA LXXVII LEGISLATURA,

ASUNTO RELACIONADO: MEDIANTE EL CUAL PRESENTAN INICIATIVA POR LA QUE SE EXPIDE LA LEY DE CIBERSERGURIDAD DEL ESTADO DE NUEVO LEÓN, LA CUAL CONSTA DE 29 ARTÍCULOS Y 5 ARTÍCULOS TRANSITORIOS.

INICIADO EN SESIÓN: Lunes 08 de Septiembre de 2025

SE TURNÓ A LA (S) COMISIÓN (ES): COMISIÓN DE JUSTICIA Y SEGURIDAD PUBLICA.

Mtro. Joel Treviño Chavira

Oficial Mayor

PODER LEGISLATIVO DEL ESTADO DE NUEVO LEÓN
SEPTUAGÉSIMA SÉPTIMA LEGISLATURA

GRUPO LEGISLATIVO morena

DIP. ITZEL SOLEDAD CASTILLO ALMANZA
PRESIDENTA DEL H. CONGRESO DEL ESTADO DE NUEVO LEÓN
PRESENTE. –

Los suscritos diputados y diputadas **CC. Mario Alejandro Soto Esquer, María Guadalupe Rodríguez Martínez, Claudia Mayela Chapa Marmolejo, Jesús Alberto Elizondo Salazar, Anylú Bendición Hernández Sepúlveda, Grecia Benavides Flores, Reyna Reyes Molina, Greta Pamela Barra Hernández, Esther Berenice Martínez Díaz y Tomás Roberto Montoya Díaz**, a la LXXVII Legislatura del H. Congreso del Estado de Nuevo León, de los Grupos Legislativos de Morena, Partido del Trabajo y Partido Verde, de conformidad con lo establecido en los artículos 87 y 88 de la Constitución Política del Estado Libre y Soberano de Nuevo León, así como lo dispuesto en lo establecido por los numerales 102, 103 y 104 del Reglamento Interior del Congreso del Estado de Nuevo León, ocurrimos a promover Iniciativa con Proyecto de Decreto por el que se expide la **Ley de Ciberseguridad del Estado *de Nuevo León***, con base en la siguiente:

EXPOSICIÓN DE MOTIVOS

La transformación digital de la economía y de los servicios públicos en Nuevo León es un hecho verificable. De acuerdo con la **ENDUTIH 2024**[1], en México 83.1% de la población de 6+ años (100.2 millones de personas) usó internet en 2024 (incremento de 1.9 pp vs 2023). Desde 2021, el uso creció 7.5 pp (de 75.6% a 83.1%), lo que confirma la aceleración de la conectividad y la expansión de la superficie de ataque digital del país.

[1] Encuesta Nacional sobre Disponibilidad y Uso de la Información en los Hogares (ENDUTIH, 2024)
https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2025/endutih/ENDUTIH_24_RR.pdf

En el plano estatal, Nuevo León se encuentra entre los estados con mayor densidad de usuarios de tecnologías de la información, tanto en el sector público como en el privado; en 2022 reportó 81.5% de hogares con internet y, para 2024, estimaciones basadas en ENDUTIH lo sitúan en torno a 83 – 84% (83.7%), manteniéndose en el grupo líder nacional. Esta magnitud de conectividad multiplica beneficios económicos y sociales, pero también incrementa la exposición a riesgos cibernéticos para personas, empresas, universidades y dependencias públicas.[2]

La amenaza es real y creciente. En 2024 se registraron en México **324 mil millones de intentos de ciberataque**, ubicándolo como uno de los países con mayor volumen en América Latina; los sectores **educativo** y **gubernamental** estuvieron entre los más hostigados. A nivel global, el **costo promedio** de una filtración de datos se ha mantenido elevado (reportes IBM 2025 – 2025)[3], con impactos de continuidad operativa, pérdida de clientes y respuesta post – incidente. Estos costos – que en contextos regionales latinoamericanos ya se miden en **millones de dólares por incidente**[4] – justifican dedicar recursos normativos y presupuestales a la **prevención** y a la **resiliencia** antes que a la sola reacción.

Nuevo León, como polo industrial y tecnológico, concentra una gran parte de la infraestructura crítica nacional, incluyendo hospitales, sistemas de transporte, servicios de agua y energía. El vacío legal en esta materia genera riesgos que afectan la protección de datos personales, el funcionamiento de servicios públicos esenciales, y la seguridad de empresas estratégicas. Si bien, México actualmente

[2] INEGI, Estadísticas a propósito del día mundial del internet, 2024 https://inegi.org.mx/contenidos/saladeprensa/aproposito/2024/EAP_DMInternet.pdf
[3] IBM, Informe del costo de una filtración de datos 2025 https://www.ibm.com/mx-es/reports/data-breach
[4] Cost of a Data Breach Report https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

cuenta con marcos federales relevantes en protección de datos personales (Ley General de Protección de Datos Personales y la Ley de Firma Electrónica Avanzada) y disposiciones sectoriales, (por ejemplo, los lineamientos de ciberseguridad financiera de CNBV), pero carece aún de una Ley General de Ciberseguridad integral que articule prevención, gestión de riesgos y respuesta para todo el ecosistema. Esta ausencia abre espacio – bajo un enfoque de competencias concurrentes – para que las entidades federativas fortalezcan sus capacidades en materias de **seguridad pública**, **protección de datos en el sector público local**, **gestión de riesgos** y **continuidad de operaciones** y coordinación intergubernamental, sin invadir la esfera federal de telecomunicaciones.

Por lo que, establecer un marco jurídico que regule la prevención, detección, gestión, mitigación y respuesta ante incidentes de ciberseguridad, a través de la creación de un Sistema Estatal de Ciberseguridad, la Agencia Estatal de Ciberseguridad, y mecanismos de colaboración interinstitucional, empresarial y ciudadana. Ya que, se resalta la necesidad de una ley de ciberseguridad con garantías de derechos humanos, proporcionalidad y controles democráticos.

A continuación, se presentan **referencias comparadas que sustentan esta propuesta:**

- Guanajuato: tiene una estrategia estatal con enfoque en ciberinteligencia.

- **España:** 1. Ley 6/2020 de Seguridad de las Redes y Sistemas de Información.

  2. INCIBE – Modelo mixto de gobernanza público – privada para cultura de ciberseguridad.

- **Colombia:** CONPES 3995/2020: Política nacional de seguridad digital con enfoque de riesgo, capacidades institucionales y colaboración multisectorial. Es un referente de política pública no penal, escalable a niveles subnacionales.[5]

- **Chile:** Proyecto de Ley Marco de Ciberseguridad (2024)[6]. Aprobó su **Ley Marco de Ciberseguridad** que crea la **Agencia Nacional de Ciberseguridad**, la cual fija obligaciones de reporte y establece un sistema nacional con coordinación público – privada. El diseño chileno muestra la convivencia de **agencias técnicas** con autonomía operativa y atribuciones claras.

- **Unión Europea** (ENISA): European Union Agency for Cybersecurity – autoridad técnica supranacional con funciones de auditoría, análisis de riesgos y respuesta rápida.

- **Brasil**: además de su ley federal de datos (LGPD, 2018), cuenta con una **Estrategia Nacional de Seguridad Cibernética** (E-Ciber) y una **Política Nacional de Ciberseguridad**, con instancias de coordinación y enfoque preventivo. Estos instrumentos muestran la utilidad de separar protección de datos (privacidad) de ciberseguridad (resiliencia), pero mantener su interoperabilidad. [7]

Si logramos expedir esta propuesta, tendremos impacto en diferentes rubros:

---

[5] Estrategia nacional de ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
[6] Ley Marco de Ciberseguridad https://www.bcn.cl/leychile/navegar?i=1202434
[7] https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

- **Social:** Protección de derechos digitales y datos personales.
- **Económico:** Fortalecimiento de la confianza en el entorno digital para inversiones.
- **Legal:** Modernización del aparato jurídico en materia de seguridad digital.
- **Técnico:** Profesionalización y coordinación de esfuerzos en el sector público.

Por lo anteriormente expuesto y fundado, me permito someter a consideración de esta H. Asamblea el presente proyecto de:

DECRETO

ÚNICO.- Se expide la Ley Ciberseguridad del Estado de Nuevo León, para quedar como sigue:

LEY DE CIBERSEGURIDAD DEL ESTADO DE NUEVO LEÓN

TÍTULO PRIMERO
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO, PRINCIPIOS Y DEFINICIONES

Artículo 1. La presente Ley es de orden público, interés social y observancia general en el Estado de Nuevo León y aplica a todos los entes públicos, empresas que operen servicios esenciales, y usuarios de tecnologías de la información.

Artículo 2. Tiene por objeto general establecer las bases para garantizar la ciberseguridad en el Estado, proteger la infraestructura crítica digital, la información pública y privada, y los derechos de las personas en el entorno digital.

Artículo 3. La presente Ley tiene como objetivos específicos:

I. Proteger los sistemas de información, redes, infraestructura crítica y activos digitales del Estado de Nuevo León contra amenazas, ataques, vulneraciones y accesos no autorizados;

II. Establecer las bases normativas y organizativas del Sistema Estatal de Ciberseguridad, promoviendo la coordinación entre autoridades, instituciones, sociedad civil y sector privado;

III. Crear e institucionalizar la Agencia Estatal de Ciberseguridad como órgano técnico especializado en la prevención, gestión y respuesta ante incidentes cibernéticos;

IV. Promover una cultura de ciberseguridad en la sociedad mediante estrategias educativas, campañas públicas y formación de capacidades en todos los niveles educativos;

V. Establecer mecanismos eficaces de reporte, monitoreo y respuesta ante incidentes cibernéticos, con especial énfasis en la protección de datos personales, derechos digitales y la seguridad de la población;

VI. Regular las obligaciones mínimas de seguridad informática de los entes públicos y empresas que operen infraestructura crítica o servicios digitales esenciales;

VII. Impulsar la colaboración internacional y nacional en materia de ciberseguridad, fomentando la interoperabilidad de políticas, protocolos y estándares técnicos;

VIII. Garantizar el respeto, protección y ejercicio de los derechos humanos en el entorno digital, especialmente en lo relativo a la privacidad, libertad de expresión y acceso seguro a la tecnología;

IX. Prevenir y mitigar los riesgos derivados del uso de tecnologías emergentes, como inteligencia artificial, internet de las cosas (IoT), computación en la nube y big data, entre otras; y

X. Establecer procedimientos administrativos y sancionadores para el incumplimiento de las disposiciones de esta Ley, sin perjuicio de las responsabilidades penales aplicables.

Artículo 4. Están sujetos a las disposiciones y cumplimiento de la presente Ley:

I. Los Poderes Ejecutivo, Legislativo y Judicial del Estado de Nuevo León, así como los organismos constitucionalmente autónomos, incluyendo sus unidades administrativas, direcciones, centros de datos, plataformas digitales y cualquier sistema informático utilizado en la prestación de servicios públicos o manejo de información;

II. Los municipios del Estado, incluyendo sus dependencias, organismos descentralizados y cualquier infraestructura digital utilizada para fines gubernamentales o administrativos;

III. Las instituciones públicas del sector educativo y de salud, así como centros de investigación que administren sistemas digitales con datos sensibles o infraestructura crítica;

IV. Las empresas, prestadores de servicios y concesionarios privados que, directa o indirectamente, operen, administren o mantengan infraestructura crítica, redes, servicios digitales esenciales, plataformas tecnológicas de uso público o servicios estratégicos en el Estado;

V. Las personas físicas o morales que desarrollen, implementen, comercialicen, integren o den mantenimiento a soluciones tecnológicas, software, dispositivos de seguridad informática o cualquier elemento relacionado con el entorno digital de entidades públicas o privadas que operen en el territorio estatal;

VI. Las organizaciones de la sociedad civil, instituciones académicas y centros de investigación que participen en proyectos, convenios o servicios en materia de tecnologías de la información, manejo de datos o ciberseguridad en el ámbito público;

VII. Cualquier persona física o moral que, mediante acción u omisión, genere o permita riesgos cibernéticos que afecten directa o indirectamente a la seguridad pública, los derechos de terceros, la privacidad, la información personal, el funcionamiento de infraestructura crítica o el entorno digital del Estado.

El cumplimiento de esta Ley no exime a los sujetos obligados de observar las disposiciones aplicables en materia de protección de datos personales, transparencia, delitos informáticos, propiedad intelectual y cualquier otra normatividad relacionada vigente en el Estado de Nuevo León o a nivel federal.

Artículo 5. Son principios rectores de esta Ley:

I. Seguridad digital;

II. Responsabilidad compartida;

III. Interoperabilidad;

IV. Proporcionalidad;

V. Protección de derechos humanos; y

VI. Colaboración público-privada.

Artículo 6. Para los efectos de la presente Ley se entederá por:

I. Ciberseguridad: Conjunto de acciones, políticas y tecnologías para proteger sistemas digitales y redes frente a amenazas;

II. Incidente de ciberseguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de los sistemas digitales;

III. Infraestructura crítica: Todo sistema, instalación, activo físico o virtual, red o servicio cuya afectación, interrupción o destrucción tenga un impacto grave en la seguridad pública, la salud, la economía, la continuidad del gobierno o el bienestar de la población del Estado de Nuevo León;

IV. Infraestructura crítica digital: Sistemas y servicios que, de ser interrumpidos, afecten significativamente la vida pública;

V. Ley: Ley de Ciberseguridad del Estado de Nuevo León;

VI. Operadores de infraestructura crítica digital: Personas físicas o morales, públicas o privadas, que administren, operen, controlen o mantengan sistemas, redes, plataformas tecnológicas o servicios cuya alteración, interrupción o destrucción pueda generar efectos adversos graves en la seguridad, salud, economía, estabilidad o servicios esenciales del Estado de Nuevo León; y

VII. Sistema: Sistema Estatal de Ciberseguridad, conjunto articulado de normas, políticas públicas, instituciones, mecanismos de coordinación, procesos técnicos y recursos humanos y tecnológicos del Estado de Nuevo León, destinado a prevenir, detectar, gestionar y responder a incidentes de ciberseguridad que afecten a personas, entidades públicas o privadas, operadores de infraestructura crítica y servicios digitales dentro del territorio estatal.

TÍTULO SEGUNDO
SISTEMA ESTATAL DE CIBERSEGURIDAD

CAPÍTULO I
INTEGRACIÓN Y FUNCIONES

Artículo 7. Se crea el Sistema Estatal de Ciberseguridad como instancia de coordinación interinstitucional, mismo que tiene por objeto coordinar, articular y supervisar las políticas públicas, estrategias, acciones y mecanismos necesarios para garantizar la seguridad del ciberespacio en el Estado de Nuevo León.

Artículo 8. El Sistema estará integrado por:

I. El Titular del Poder Ejecutivo;
II. La Agencia Estatal de Ciberseguridad;
III. La Secretaría de Seguridad Pública;
IV. La Fiscalía General del Estado;
V. Un representante del Poder Judicial;
VI. Un representante del Poder Legislativo;
VII. Los Presidentes Municipales de los Municipios del Área Metropolitana;
VIII. Tres representantes de la academia;
IX. Dos representantes del sector privado; y
X. Tres representantes de organizaciones de la sociedad civil.

Artículo 9. Para el cumplimiento de sus fines, el Sistema, tendrá las siguientes funciones:

I. Diseñar, actualizar y evaluar la Estrategia Estatal de Ciberseguridad, en coordinación con las dependencias, organismos y sectores involucrados;

II. Establecer criterios, estándares técnicos, lineamientos y protocolos de prevención, detección, análisis, respuesta y recuperación ante incidentes de ciberseguridad, aplicables a los sujetos obligados por esta Ley;

III. Fomentar la creación y operación de Centros de Respuesta a Incidentes Cibernéticos en instituciones públicas y privadas, así como garantizar su interoperabilidad con la Agencia Estatal de Ciberseguridad;

IV. Coordinar y supervisar el cumplimiento de las obligaciones establecidas en esta Ley por parte de las dependencias y entidades públicas, y promover buenas prácticas en el sector privado y académico;

V. Establecer canales permanentes de colaboración y cooperación técnica con el Gobierno Federal, entidades federativas, municipios, organismos internacionales, instituciones académicas y actores del sector privado en materia de ciberseguridad;

VI. Promover la educación, capacitación y sensibilización en materia de ciberseguridad, tanto en el sector público como en la población general, con perspectiva de derechos humanos, inclusión digital y enfoque preventivo;

VII. Emitir recomendaciones y alertas tempranas sobre amenazas cibernéticas que puedan afectar a la infraestructura crítica, la información pública, el patrimonio digital o los derechos de las personas;

VIII. Realizar diagnósticos periódicos sobre el estado de la ciberseguridad en el Estado, incluyendo evaluaciones de riesgo, niveles de madurez digital y brechas en capacidades institucionales;

IX. Integrar un registro estatal de incidentes cibernéticos, con fines estadísticos, preventivos y de mejora institucional, respetando en todo momento la confidencialidad y la legislación en materia de protección de datos personales;

X. Fomentar la participación ciudadana, empresarial, académica y tecnológica en el diseño y evaluación de políticas públicas de ciberseguridad, mediante observatorios, consejos consultivos u otros mecanismos participativos;

XI. Elaborar informes anuales sobre el estado que guarda la ciberseguridad en el Estado de Nuevo León, incluyendo avances, retos y recomendaciones, los cuales deberán ser públicos y remitidos al Poder Legislativo;

XII. Coadyuvar con las autoridades competentes en la prevención de delitos informáticos, sin menoscabo de sus competencias ni de las disposiciones penales aplicables;

XIII. Impulsar la innovación, investigación y desarrollo tecnológico en materia de ciberseguridad, así como la creación de capacidades técnicas especializadas en instituciones estatales; y

XIV. Las demás que sean necesarias para el cumplimiento de los fines de esta Ley o que le sean conferidas por otras disposiciones normativas.

TÍTULO TERCERO
AGENCIA ESTATAL DE CIBERSEGURIDAD

CAPÍTULO I
NATURALEZA Y ATRIBUCIONES

Artículo 10. Se crea la Agencia Estatal de Ciberseguridad como una unidad administrativa de la Fiscalía General, cuyo objeto es planear, coordinar, ejecutar y evaluar las políticas públicas en materia de ciberseguridad del Estado de Nuevo León.

Artículo 11. La Agencia desarrollará sus funciones bajo los siguientes principios:

I. Proactividad tecnológica y anticipación de riesgos;
II. Enfoque de derechos humanos y protección de datos;
III. Transparencia, rendición de cuentas y mejora continua;
IV. Neutralidad tecnológica e interoperabilidad; y
V. Confianza digital, resiliencia cibernética y soberanía tecnológica.

Artículo 12. La Agencia contará, al menos, con las siguientes unidades administrativas:

I. Dirección General;
II. Unidad de Análisis de Riesgos y Prospectiva Tecnológica;
III. Centro Estatal de Respuesta a Incidentes Cibernéticos;
IV. Dirección de Certificación, Normas Técnicas y Protocolos;
V. Dirección de Cultura Digital y Formación Ciudadana;
VI. Dirección de Supervisión y Cumplimiento; y
VII. Dirección de Vinculación Interinstitucional e Internacional.

Artículo 13. La Agencia tendrá, entre otras, las siguientes atribuciones:

I. Implementar y operar la Estrategia Estatal de Ciberseguridad, en coordinación con las dependencias del Sistema Estatal;
II. Establecer, mantener y operar el Centro Estatal de Respuesta a Incidentes Cibernéticos, para la atención, análisis y mitigación de amenazas cibernéticas;
III. Emitir normas técnicas, directrices, manuales, metodologías y lineamientos sobre buenas prácticas en ciberseguridad para entidades públicas y privadas sujetas a esta Ley;

IV. Coordinar auditorías de cumplimiento en materia de ciberseguridad, protección de datos, continuidad operativa y resiliencia digital;

V. Gestionar la vigilancia de amenazas cibernéticas en tiempo real, incluyendo la detección de vulnerabilidades críticas, malware, botnets, ransomware, ataques de denegación de servicio (DDoS) y campañas de desinformación digital;

VI. Diseñar, aplicar y validar protocolos de ciberseguridad para infraestructura crítica digital, así como para los operadores identificados como estratégicos, conforme al registro estatal, y coordinar mecanismos de respaldo y recuperación ante desastres digitales;

VII. Evaluar, certificar y capacitar a personal técnico, funcionarios públicos y especialistas del sector privado en estándares internacionales de seguridad;

VIII. Desarrollar e implementar campañas de cultura digital, alfabetización cibernética, protección infantil en entornos digitales, ciberacoso, suplantación de identidad, fraudes financieros y manipulación algorítmica;

IX. Fomentar la innovación, la investigación aplicada y la formación de talento especializado en ciberseguridad mediante alianzas con universidades, empresas y centros de investigación del país y del extranjero;

X. Establecer canales de cooperación y acuerdos con agencias homólogas nacionales e internacionales;

XI. Emitir alertas de seguridad digital y recomendaciones periódicas para prevenir riesgos masivos, campañas de phishing, ingeniería social y otras amenazas emergentes;

XII. Proponer al Ejecutivo del Estado proyectos de reforma legal, presupuestaria o institucional en materia de ciberseguridad y soberanía digital;

XIII. Operar un registro estatal de incidentes de ciberseguridad, con clasificaciones por nivel de impacto, sector, origen del ataque, consecuencias y medidas tomadas, respetando la confidencialidad de datos y derechos fundamentales;

XIV. Evaluar anualmente los niveles de madurez digital y ciberresiliencia de las instituciones del gobierno estatal y organismos descentralizados, y proponer medidas de mejora;

XV. Imponer sanciones administrativas, conforme a la presente Ley, en caso de incumplimiento de medidas mínimas de ciberseguridad en entes obligados; y

XVI. Las demás que le confieran esta Ley, su reglamento o disposiciones jurídicas aplicables.

TÍTULO CUARTO
PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 14. La Agencia elaborará un padrón estatal de infraestructura digital crítica.

Artículo 15. La protección de infraestructura crítica se regirá por los siguientes principios:

I. Prevención: Identificación y mitigación anticipada de riesgos;

II. Resiliencia: Capacidad de recuperación rápida ante incidentes;

III. Continuidad: Garantía de funcionamiento permanente de servicios esenciales;

IV. Coordinación: Interoperabilidad entre autoridades, operadores y sector privado; y

V. Confidencialidad, integridad y disponibilidad de la información.

CAPÍTULO II
IDENTIFICACIÓN Y CLASIFICACIÓN

Artículo 16. La Agencia Estatal de Ciberseguridad identificará y mantendrá actualizado un Catálago Estatal de Infraestructura Crítica que, como mínimo, incluirá:

I. Energía eléctrica, hidrocarburos y combustibles;
II. Agua potable y saneamiento;
III. Telecomunicaciones y servicios digitales;
IV. Salud pública y hospitales;
V. Transporte y logística;
VI. Finanzas y sistema de pagos;
VII. Gobierno digital y bases de datos estratégicas; y
VIII. Seguridad pública y sistemas de emergencia.

Artículo 17. La Agencia establecerá niveles de prioridad alto, medio o bajo en función de:

I. Alcance geográfico del impacto;
II. Magnitud de la población afectada;
III. Dependencia tecnológica del sistema; y
IV. Potencial de daño económico, social o ambiental.

CAPÍTULO III
MEDIDAS DE PROTECCIÓN Y RESPUESTA

Artículo 18. Obligaciones específicas de los operadores de infraestructura crítica digital. Quienes administren o gestionen infraestructura crítica tendrán las siguientes obligaciones:

I. Inscribirse en el Registro Estatal de Infraestructura Crítica Digital, en los términos que determine la Agencia;
II. Implementar sistemas de gestión de ciberseguridad alineados con normas internacionales;
III. Implementar políticas, herramientas, controles técnicos y administrativos de ciberseguridad conforme a los estándares emitidos por la Agencia;
IV. Establecer protocolos de monitoreo y detección temprana de incidentes;
V. Notificar a la Agencia, de manera inmediata y obligatoria, cualquier incidente de ciberseguridad que pueda afectar la continuidad de servicios esenciales, la seguridad pública o la información confidencial;
VI. Permitir la realización de auditorías técnicas, revisiones de cumplimiento y evaluaciones de riesgo por parte de la Agencia;
VII. Colaborar en ejercicios de simulación de incidentes cibernéticos organizados por el Sistema Estatal de Ciberseguridad;
VIII. Designar un Enlace de Ciberseguridad responsable de la comunicación institucional con la Agencia;
IX. Cumplir con los lineamientos que en materia de protección de datos personales y continuidad operativa sean determinados por otras autoridades competentes; y
X. Las demás que les sean aplicables conforme a esta Ley y su reglamento.

Artículo 19. Todo operador de infraestructura crítica deberá contar con un Plan de Continuidad Operativa y un Plan de Recuperación ante Desastres que incluyan:

I. Escenarios de ataque cibernético y respuesta inmediata;
II. Procedimientos para restauración de servicios;
III. Mecanismos de comunicación con la población afectada; y
IV. Protocolos de respaldo de información crítica.

CAPÍTULO IV
COORDINACIÓN Y APOYO INTERINSTITUCIONAL

Artículo 20. La Agencia Estatal de Ciberseguridad establecerá canales de cooperación con:

I. Autoridades federales;
II. Dependencias estatales y municipales;
III. Organismos reguladores sectoriales; y
IV. Entidades privadas con funciones estratégicas.

Artículo 21. Al menos una vez al año, se realizarán simulacros intersectoriales para poner a prueba los protocolos de protección, respuesta y recuperación.

CAPÍTULO V
SANCIONES Y RESPONSABILIDADES DE LOS OPERADORES

Artículo 22. El incumplimiento por parte de los operadores de infraestructura crítica en la adopción de las medidas establecidas en este Título podrá dar lugar a:

I. Multas administrativas;
II. Suspensión temporal de licencias o concesiones; y
III. Responsabilidad civil o penal en los términos de la legislación aplicable.

TÍTULO QUINTO
PARTICIPACIÓN CIUDADANA Y CULTURA DIGITAL

CAPÍTULO I
EDUCACIÓN Y CULTURA DIGITAL

Artículo 23. La Agencia deberá coordinarse con la Secretaría de Educación para incluir contenidos de ciberseguridad en educación básica y media.

CAPÍTULO II
DENUNCIA CIUDADANA

Artículo 24. Se habilitará una plataforma para reportar incidentes y fraudes digitales.

TÍTULO SEXTO
RESPONSABILIDADES, SANCIONES Y PROCEDIMIENTOS

CAPÍTULO I
SANCIONES ADMINISTRATIVAS

Artículo 25. Las personas físicas o morales que incumplan las obligaciones establecidas podrán ser sancionadas conforme a la gravedad del incidente:

I. Amonestación pública o privada;
II. Multa de 200 a 10,000 veces el valor diario de la UMA;
III. Suspensión, remoción o inhabilitación del cargo en el caso de servidoras o servidores públicos;

IV. Cancelación de licencias, permisos o registros en el caso de prestadores de servicios digitales; y

V. Responsabilidad administrativa conforme a otras leyes aplicables.

CAPÍTULO II
RESPONSABILIDADES PENALES Y CIVILES

Artículo 26. Cuando las conductas previstas en esta Ley constituyan delitos o causen daño moral o patrimonial, deberán denunciarse ante la autoridad competente para que se ejerza acción penal o civil conforme a las leyes aplicables.

CAPÍTULO III
DE LOS CRITERIOS PARA LA IMPOSICIÓN DE SANCIONES

Artículo 27. Se considerarán omisiones graves aquellas conductas que, por su naturaleza o consecuencias, pongan en riesgo significativo la seguridad de los sistemas, datos o infraestructuras críticas, incluyendo de manera enunciativa, más no limitativa:

I. La falta de implementación de medidas mínimas de ciberseguridad previstas en esta Ley y en las disposiciones reglamentarias, por parte de entidades obligadas;

II. No reportar de manera inmediata incidentes de ciberseguridad a la Agencia Estatal de Ciberseguridad cuando se trate de vulneraciones que comprometan datos personales, información clasificada o infraestructura crítica;

III. No atender las recomendaciones u órdenes emitidas por la Agencia Estatal de Ciberseguridad en el plazo establecido;

IV. La ausencia de protocolos internos de respuesta ante incidentes cibernéticos en instituciones públicas y privadas obligadas por esta Ley;

V. Negarse a colaborar con las autoridades competentes en la investigación de incidentes de ciberseguridad; y

VI. Desactivar o manipular sistemas de seguridad informática de manera intencional o negligente, afectando la integridad, disponibilidad o confidencialidad de la información.

Artículo 28. Para la determinación de la sanción correspondiente, la autoridad competente tomará en cuenta:

I. Circunstancias atenuantes:

a) Haber adoptado voluntariamente medidas correctivas inmediatas para mitigar el daño;

b) Colaborar proactivamente con la Agencia Estatal de Ciberseguridad y otras autoridades en la investigación del incidente; y

c) Haber implementado programas internos de capacitación y prevención en ciberseguridad previos al incidente.

II. Circunstancias agravantes:

a) Reincidencia en la conducta infractora en un período menor a dos años;

b) Ocultar información relevante o falsear datos relacionados con el incidente;

c) Que la infracción afecte infraestructura crítica o ponga en riesgo la seguridad pública; y

d) Que el incidente haya tenido impacto en servicios esenciales de salud, seguridad, justicia, energía, agua, transporte o telecomunicaciones.

CAPÍTULO IV

DE LAS AUTORIDADES COMPETENTES PARA SANCIONAR

Artículo 29. Son autoridades competentes para imponer las sanciones previstas en esta Ley:

I. La Agencia Estatal de Ciberseguridad, respecto de infracciones administrativas cometidas por particulares y entes públicos sujetos a esta Ley;
II. La Secretaría de Seguridad del Estado, cuando las conductas constituyan riesgos o amenazas a la seguridad pública derivadas de ataques cibernéticos;
III. La Fiscalía General de Justicia del Estado, en los casos en que las conductas configuren delitos conforme al Código Penal del Estado o legislación federal aplicable;
IV. La Contraloría y Transparencia Gubernamental del Estado, en casos de responsabilidad administrativa de servidores públicos; y
V. Las autoridades municipales competentes, respecto a infracciones en el ámbito de su jurisdicción, de conformidad con los convenios de colaboración que se suscriban.

ARTÍCULOS TRANSITORIOS

ARTÍCULO PRIMERO. - El presente Decreto, entrará en vigor al siguiente día de su publicación en el Periódico Oficial del Estado de Nuevo León.

ARTÍCULO SEGUNDO.- El Poder Ejecutivo del Estado deberá emitir el Reglamento de esta Ley en un plazo no mayor a 120 días naturales.

ARTÍCULO TERCERO.- El Sistema Estatal de Ciberseguridad deberá integrarse en un plazo máximo de 90 días a partir de la entrada en vigor del presente Decreto.

ARTÍCULO CUARTO.- La Agencia Estatal de Ciberseguridad deberá integrarse en un plazo máximo de 90 días a partir de la entrada en vigor del presente Decreto.

ARTÍCULO QUINTO.- Se contará con un plazo no mayor a 90 días naturales a partir de la publicación del presente Decreto en el Periódico Oficial del Estado, para realizar las modificaciones necesarias a las leyes secundarias.

H. CONGRESO DEL ESTADO
OFICIALIA MAYOR
RECIBIDO
04 SEP 2025
DEPARTAMENTO
OFICIALIA DE PARTES
MONTERREY, N.L.

Atentamente

Monterrey, Nuevo León a 04 de septiembre del 2025

DIPUTADO MARIO ALEJANDRO SOTO ESQUER

COORDINADOR DE LA BANCADA DE MORENA

DIPUTADA MARÍA GUADALUPE RODRÍGUEZ MARTÍNEZ

COORDINADORA DE LA BANCADA DE PARTIDO DEL TRABAJO

DIPUTADA CLAUDIA MAYELA CHAPA MARMOLEJO

COORDINADORA DE LA BANCADA DE PARTIDO VERDE

DIPUTADO JESÚS ALBERTO ELIZONDO SALAZAR

LXXVII
PODER LEGISLATIVO DEL ESTADO DE NUEVO LEÓN
SEPTUAGÉSIMA SÉPTIMA LEGISLATURA

PT

VERDE

GRUPO LEGISLATIVO
morena

DIPUTADA GRETA PAMELA BARRA HERNÁNDEZ

DIPUTADA GRECIA BENAVIDES FLORES

DIPUTADA ANYLU BENDICIÓN HERNÁNDEZ SEPÚLVEDA

DIPUTADA ESTHER BERENICE MARTÍNEZ DÍAZ

DIPUTADO TOMÁS ROBERTO MONTOYA DÍAZ

DIPUTADA REYNA REYES MOLINA

H. CONGRESO DEL ESTADO
OFICIALIA MAYOR
RECIBIDO
04 SEP 2025
11:43h
DEPARTAMENTO
OFICIALIA DE PARTES
MONTERREY, N.L.