AÑO:2026 EXPEDIENTE: 20997/LXXVII

H. Congreso del Estado de Nuevo León

LXXVII Legislatura

PROMOVENTE: C. DIP. SANDRA ELIZABETH PÁMANES ORTIZ, COORDINADORA DE MOVIMIENTO CIUDADANO DE LA LXXVII LEGISLATURA.

ASUNTO RELACIONADO: PRESENTA INICIATIVA POR LA QUE SE EXPIDE LA LEY DE CIBERSEGURIDAD DEL ESTADO DE NUEVO LEÓN, LA CUAL CONSTA DE 58 ARTÍCULOS Y 4 ARTÍCULOS TRANSITORIOS.

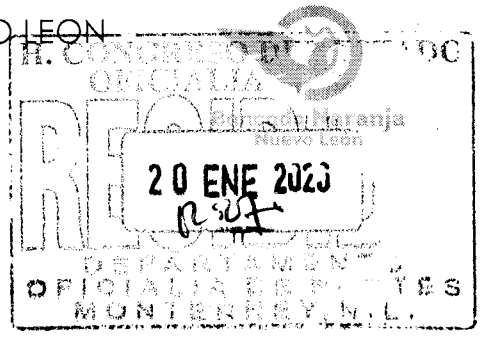
INICIADO EN SESIÓN: 21 DE ENERO DEL 2026

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

Mtro. Joel Treviño Chavira

Oficial Mayor

H. CONGRESO DEL ESTADO DE NUEVO LEON
LXXVII Legislatura
GRUPO LEGISLATIVO DEL PARTIDO
MOVIMIENTO CIUDADANO



PRESIDENCIA DE LA MESA DIRECTIVA DEL
H. CONGRESO DEL ESTADO DE NUEVO LEÓN
P R E S E N T E.-

Quienes suscriben, Diputadas **Sandra Elizabeth Pámanes Ortiz**, Dip. Ana Melisa Peña Villagomez, Dip. Paola Cristina Linares López, Dip. Marisol González Elías, Diputados Dip. Glen Alan Villarreal Zambrano, Dip. Baltazar Gilberto Martínez Ríos, Dip. José Luis Garza Garza, Dip. Armando Víctor Gutiérrez Canales, Dip. Mario Alberto Salinas Treviño, integrantes del Grupo Legislativo de Movimiento Ciudadano de la LXXVII Legislatura del H. Congreso del Estado de Nuevo León; con fundamento en los artículos 56 fracción III, 87 y 88 de la Constitución Política del Estado Libre y Soberano de Nuevo León; los artículos 102, 103 y 104 del Reglamento para el Gobierno Interior del Congreso del Estado, someto a la consideración de esta Honorable Asamblea, la siguiente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY DE CIBERSEGURIDAD DEL ESTADO DE NUEVO LEÓN.**

De acuerdo al artículo 88 de la Constitución Política del Estado Libre y Soberano de Nuevo León presentamos de nueva cuenta la presente iniciativa para su estudio, análisis y dictamen, misma que fue dada de baja sin el estudio correspondiente con fundamento en el artículo 46 del Reglamento para el Gobierno Interior del Congreso dentro del expediente **19308/LXXVII.**

EXPOSICIÓN DE MOTIVOS

El ciberespacio es real, las amenazas cibernéticas en y a través del mismo con un impacto en el mundo físico también, y en el centro de todo están las sociedades, las empresas, los gobiernos, sus derechos, sus interacciones y sus logros. Las amenazas cibernéticas cada vez más frecuentes, complejas y destructivas atentan contra bienes jurídicamente tutelados y derechos como la vida, la integridad, la salud, el patrimonio, los activos de información, la privacidad, la reputación e incluso inciden en la opinión pública a través de información falsa, lo que crea desinformación, perjudicando a niñas, niños, adultos, empresas, instituciones gubernamentales y relaciones internacionales.

La dependencia tecnológica y los beneficios de su adopción para los gobiernos, empresas y sociedad son hechos notorios ampliamente comprobados local como internacionalmente, por lo que no es necesario su sustento, máxime que ello exacerba los riesgos que representan las amenazas cibernéticas, las cuales constituyen un mercado global emergente, en consolidación y ampliamente lucrativo.

Hoy en día resulta complejo medir y cuantificar las consecuencias directas e indirectas que puede tener un ataque cibernético a todas las actividades y servicios gubernamentales, sean infraestructuras críticas y/o servicios esenciales o no, constituyendo las instituciones gubernamentales del Estado y sus municipios (orden estatal y municipal) una prioridad en su protección, en virtud de los servicios de gobierno que se prestan a la ciudadanía a través de los poderes ejecutivo, legislativo, judicial y órganos autónomos.

Garantizar la seguridad cibernética de las instituciones gubernamentales en el Estado y sus municipios es un asunto de seguridad pública que no puede postergarse más, y es en el Estado en donde debe hacerse un esfuerzo histórico y sin precedentes por parte del Poder Legislativo para contar con la primera legislación en materia de ciberseguridad.

Impacto internacional

Es de resaltar que desde el T-MEC, mismo que fue establecido como un tratado "que aborde los retos y las oportunidades futuras del comercio y la inversión, y contribuir con el fomento de sus respectivas prioridades en el tiempo".[1] En este sentido, el "Capítulo 19 Comercio Digital", en su artículo 19.15, establece un apartado titulado "Ciberseguridad", en el cual se aprecia lo siguiente:

[1] DECRETO Promulgatorio del Protocolo por el que se Sustituye el Tratado de Libre Comercio de América del Norte por el Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá, hecho en Buenos Aires, el treinta de noviembre de dos mil dieciocho [...] Publicado en el Diario Oficial de la Federación el 29 de junio de 2020. Disponible en: http://dof.gob.mx/2020/SRE/TMEC290620.pdf

Artículo 19.15: Ciberseguridad

1. Las Partes reconocen que las amenazas a la ciberseguridad menoscaban la confianza en el comercio digital. Por consiguiente, las Partes procurarán:

(a) desarrollar las capacidades de sus respectivas entidades nacionales responsables de la respuesta a incidentes de ciberseguridad; y

(b) fortalecer los mecanismos de colaboración existentes para cooperar en identificar y mitigar las intrusiones maliciosas o la diseminación de códigos maliciosos que afecten a las redes electrónicas y utilizar esos mecanismos para tratar rápidamente los incidentes de ciberseguridad, así como para el intercambio de información para el conocimiento y las mejores prácticas.

2. Dada la naturaleza cambiante de las amenazas a la ciberseguridad, las Partes reconocen que los enfoques basados en riesgos pueden ser más efectivos que la regulación prescriptiva para tratar aquellas amenazas. En consecuencia, cada Parte procurará emplear y alentar a las empresas dentro de su jurisdicción a utilizar enfoques basados en riesgos que dependan de normas consensuadas y mejores prácticas de gestión de riesgos para identificar y proteger contra los riesgos de ciberseguridad y detectar, responder y recuperarse de eventos de ciberseguridad.

De lo establecido en el T-MEC se puede observar que el Estado mexicano reconoció que las amenazas a la ciberseguridad menoscaban la confianza, en este caso, **en el comercio digital**, no obstante, el sector gubernamental federal y local no son ajenos a las amenazas a la ciberseguridad. En este sentido, el Estado debe coadyuvar en el ámbito de su competencia a efecto de desarrollar capacidades y mecanismos de colaboración gubernamentales para tratar rápidamente los incidentes de ciberseguridad, en concordancia con lo establecido por el T-MEC y dada su intervención con el sector comercial establecido en el Estado.

Ámbito en el Estado de Nuevo León

En el Estado de Nuevo León, la Policía Cibernética es el ente auxiliar para investigar los delitos cometidos en las redes como son la extorsión, amenazas, difamación, y por supuesto fraude y usurpación de identidad.

La policía cibernética de Nuevo León atiende:

- Extorsión

- Amenazas
- Difamación
- Fraude
- Usurpación de identidad
- Pornografía infantil
- Sexting
- Acoso
- "Grooming" (acoso a menores de edad)

El delito informático se refiere a cualquier actividad ilegal que se comete utilizando tecnología informática o redes de comunicación. Esto puede incluir el acceso no autorizado a sistemas informáticos, el robo de información confidencial, el fraude en línea, el acoso cibernético y la difusión de contenido ilegal. Los delitos informáticos son castigados por la ley y pueden tener graves consecuencias legales para los infractores.

DELITOS DE FRAUDE Y SUPLANTACIÓN DE IDENTIDAD

Actualmente en el Estado, y de Acuerdo a datos de la Secretaría de Seguridad se revela que en promedio se reciben al día entre 35 y 50 reportes de personas afectadas.

La mayoría de las incidencias son por fraudes, mientras que en segundo lugar se encuentra el delito de suplantación de identidad.

Las cifras de la Secretaría de Seguridad apenas permiten observar una parte del fenómeno, pues provienen únicamente de las solicitudes de ayuda de la ciudadanía a través de las redes sociales de la Policía Cibernética.

Es señalar que la Fiscalía no cuenta una estadística pública para determinar si la incidencia se contempla o no cometido en el ciberespacio, también en el Poder Judicial no existen detalles sobre sentencias a criminales que operan en la red.

En Nuevo León ha experimentado un alarmante incremento de **422%** en los delitos cibernéticos en el último año, especialmente los de fraudes y extorsiones.

Mientras que para 2022 se registraron 1,557 ciberdelitos de fraude y extorsión, para 2023, de acuerdo a la más reciente medición del Instituto Nacional de Estadística y Geografía (INEGI), fue de 8,138 casos.

Según datos recientes, estos tipos de delitos han aumentado un **448% en el último año a nivel nacional**, pero además es el ciberdelito más cometido en la región, entre cuyas modalidades se encuentra el "secuestro virtual", el "fraude nigeriano", así como las falsas entregas de paquetes, entre otros.

Los extorsionadores telefónicos han encontrado en los regiomontanos un blanco fácil, utilizando diversas tácticas para engañar y extorsionar a sus víctimas.

Entre las modalidades más comunes se encuentran los secuestros virtuales, donde los delincuentes simulan haber secuestrado a un familiar para exigir grandes sumas de dinero.

Además de los secuestros virtuales, otras modalidades de fraude incluyen la supuesta entrega de paquetería, donde los estafadores se hacen pasar por empleados de empresas de mensajería para obtener información personal y financiera de sus víctimas.

Estos métodos han sido reportados por diversos testimonios compartidos, destacando la creatividad y persistencia de los delincuentes.

Expertos en seguridad cibernética advierten que la población más propensa a caer en estos engaños son los menores de edad.

CASOS DE CIBER ACOSO

Uno de cada cinco menores tiene contacto con pedófilos o depredadores sexuales, pero solo el 25% de las víctimas delatan la agresión a sus madres, padres o tutores, esto según la Asociación Mexicana de Internet.

El tiempo que niñas, niños y adolescentes pasan en línea aumenta el riesgo de sufrir ciberacoso, y en Nuevo León, esta preocupación es aún más urgente.

Según datos ofrecidos en 2020 por la Policía Cibernética de Nuevo León, en promedio **reciben 12 reportes diarios por presunta vulneración** de derechos de infancias y adolescencias, siendo **Guadalupe, Monterrey y Juárez los municipios más afectados por el ciberacoso.**

En esta materia, **proteger a las infancias es primordial,** pues, aunque el **78% de los padres manifiestan preocupación por el ciberacoso**, solo el **16% sabe cómo establecer reglas y límites en el uso de dispositivos digitales.**

De igual forma, es crucial **impulsar la cultura de la denuncia para generar mayor visibilidad** y encontrar soluciones que **prevengan estas problemáticas** tanto en la "digitalidad" como en la vida real de las infancias.

El ciberacoso contra niñas, niños y adolescentes es algo más que una broma pesada en redes sociales o plataformas de videojuegos, pues implica un comportamiento criminal

que rápidamente puede escalar a hostigamiento, discriminación y varias formas de violencia, llegando incluso a exigir contenido sexual y a extorsionar a las víctimas.

"HACKEO" DE INFORMACIÓN (FÍSCALÍA DE NL Y "WHATSAPP" DEL GOBERNADOR DEL ESTADO)

El pasado mes de noviembre de 2024 la Fiscalía General de Justicia de Nuevo León confirmó el robo de archivos que sufrió a principios de este 2024, el cual se reveló en redes sociales en los últimos días.

La autoridad señaló que, ante la detección de actividad inusual en sus servidores informáticos, **se inició en marzo de 2024** una carpeta de investigación para esclarecer los hechos y dar con los responsables.

Así mismo es de señalar que el pasado 05 de enero del presente año (2025) se informó por tarde de la Oficina de Comunicación del Estado ignorar mensajes procedentes del número telefónico usado por el Gobernador Samuel García, ya que fue víctima de "hackeo" de su número de la aplicación de "whatsapp".

Es por ello que ante la importancia de generar seguridad ciudadana en el Ciberespacio es que consideramos prioritario presentar la presente Ley para prevenir, investigar y en su caso sancionar cualquier daño a la seguridad cibernética en el Estado.

En mérito de lo expuesto, se somete a la consideración de esta Honorable asamblea, el siguiente proyecto de:

DECRETO

ÚNICO. –Se **expide** la **LEY DE CIBERSEGURIDAD DEL ESTADO DE NUEVO LEÓN**, que consta de 58 artículos y 4 artículos transitorios, para quedar como sigue:

LEY DE CIBERSEGURIDAD DEL ESTADO DE NUEVO LEÓN

TÍTULO PRIMERO
DISPOSICIONES GENERALES

Capítulo Único
Objeto

Artículo 1. La presente Ley es de orden público y tiene por objeto garantizar la seguridad cibernética del Estado de Nuevo León y sus municipios.

La seguridad cibernética será una herramienta utilizada y aprovechada para garantizar la gobernabilidad del Estado y como una capacidad de alto nivel para coadyuvar en el desarrollo tecnológico, político, económico y social en el Estado de Nuevo León y sus municipios.

Finalidades

Artículo 2. La seguridad cibernética en el Estado tiene como finalidades garantizar:

I. El cumplimiento de las facultades, atribuciones y obligaciones de ley de las Autoridades, que en todo o en parte hagan uso de las tecnologías de la información y comunicación;

II. La disponibilidad, continuidad y confiabilidad de los procedimientos, trámites y servicios públicos de las Autoridades, que en todo o en parte hagan uso de las tecnologías de la información y comunicación;

III. La integridad, confidencialidad, disponibilidad, autenticidad y no repudio de la información en posesión de las Autoridades;

IV. La protección, funcionamiento, confiabilidad, rendimiento y disponibilidad de las tecnologías de la información y comunicación de las Autoridades o en su posesión;

V. La seguridad de servidores públicos, empresas y ciudadanos, cuya información esté en posesión de las Autoridades, y

VI. Generar y fortalecer la confianza digital de los servidores públicos, empresas y ciudadanos en los procedimientos, trámites y servicios públicos electrónicos a cargo de las Autoridades.

Las finalidades anteriores son críticas y esenciales para el adecuado funcionamiento de las Autoridades del Estado.

Ámbito de aplicación

Artículo 3. Todas las autoridades, dependencias, entidades, órganos y organismos de los Poderes Ejecutivo, Legislativo y Judicial, los municipios, organismos descentralizados o desconcentrados, organismos autónomos, tribunales administrativos, fideicomisos y fondos públicos del orden estatal y municipal del Estado están obligados a cumplir con esta Ley.

El cumplimiento de la presente Ley es independiente del cumplimiento de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Contenido

Artículo 4. Para cumplir con el objeto de la presente Ley:

I. Se establecen obligaciones para las Autoridades a efecto de garantizar su seguridad cibernética, de los servidores públicos, de los prestadores de servicios y de los ciudadanos;

II. Se crea la autoridad encargada de liderar y coordinar los esfuerzos en materia de ciberseguridad en el Estado;

III. Se crea un equipo de inteligencia y respuesta a incidentes de seguridad cibernética;

IV. Se crean las unidades de ciberseguridad como áreas encargadas de garantizar la seguridad cibernética de las autoridades;

V. Se crea la Fiscalía Especializada en Delitos Cibernéticos como parte de la Fiscalía General de Justicia del Estado.

VI. Se establece el tipo de falta administrativa para conductas que contravengan la presente Ley, y

VII. Se establecen los delitos en contra de la ciberseguridad del Estado.

Definiciones

Artículo 5. Para los efectos de esta Ley se entenderá por:

I. **Amenaza cibernética**: cualquier circunstancia, situación, hecho, acción, omisión, incidente, evento de TIC y cualquier otra violación a políticas en materia de ciberseguridad con el potencial de dañar, perturbar, vulnerar, comprometer o poner en riesgo el cumplimiento de las finalidades previstas en el artículo segundo de la presente Ley;

II. **Ataque**: la materialización de una amenaza cibernética;

III. **Autoridades:** todas las autoridades, dependencias, entidades, órganos y organismos de los Poderes Ejecutivo, Legislativo y Judicial, los municipios, organismos descentralizados o desconcentrados, organismos autónomos,

tribunales administrativos, fideicomisos y fondos públicos del orden estatal y municipal del Estado;

IV. **Autoridad Investigadora**: la referida en el artículo 3, de la Ley de Responsabilidades Administrativas del Estado de Nuevo León

V. **Ciberseguridad o seguridad cibernética:**

A. Todas las actividades necesarias para preservar la operación, funcionamiento, disponibilidad, confiabilidad y continuidad de todas las actividades, procedimientos, trámites y servicios públicos de las Autoridades que dependan y/o hagan uso de las TIC en forma parcial o total o en cualquier parte de su proceso;

B. Todas las actividades necesarias para la protección de las TIC de las Autoridades o en su posesión, de sus usuarios y de terceros de amenazas cibernéticas y ataques;

C. La capacidad de preservar, al menos, la integridad, disponibilidad, confidencialidad, autenticidad y no repudio de la información en posesión de las Autoridades;

D. Cualquier actividad necesaria para prevenir, mitigar o suprimir amenazas cibernéticas, ataques o sus impactos, y

E. Cualquier otra actividad que sea necesaria para cumplir con las finalidades previstas en el artículo segundo de la presente Ley.

VI. **Dictamen de ciberseguridad:** la opinión técnica emitida por la Unidad de Ciberseguridad, en la que hace constar que todo proyecto, actividad, procedimiento, trámite y servicio de las Autoridades que en todo o en parte haga o pretenda hacer uso de las TIC cumple o no con los requisitos mínimos de ciberseguridad. Este dictamen aplica a cualquier contratación de servicios de TIC y de ciberseguridad.

VII. **EIRIC:** el Equipo de Inteligencia y Respuesta a Incidentes de Ciberseguridad del Estado;

VIII. **Estado:** el Estado Libre y Soberano de Nuevo León;

IX. **Evento de TIC:** cualquier suceso o acontecimiento en una TIC;

X. **Gestión de riesgos:** la identificación, valoración y ejecución de acciones para el control y mitigación del riesgo;

XI. **Ley**: la Ley de Ciberseguridad del Estado de Nuevo León;

XII. **Política general de ciberseguridad**: documento que establece los controles en materia de ciberseguridad necesarios para garantizar las finalidades previstas en el artículo segundo de la presente Ley;

XIII. **Política sectorial de ciberseguridad:** política complementaria a la política general de ciberseguridad, especializada en un sector gubernamental, procedimiento, trámite o servicio público específico;

XIV. **Proveedores tecnológicos:** personas físicas o morales que presten servicios de TIC y de ciberseguridad;

XV. **Resiliencia:** las capacidades de cualquier tipo para anticiparse, resistir, adaptarse, recuperarse y reducir la duración o impacto de una amenaza cibernética o ataque;

XVI. **Riesgo:** la posibilidad de materialización de una amenaza cibernética y sus consecuencias;

XVII. **TIC:** las Tecnologías de la Información y Comunicación, que comprenden, al menos, todo tipo de tecnología en cualquier soporte para recolectar, almacenar, procesar, convertir, proteger, transferir, recuperar y/o cualquier otra interacción o actividad con cualquier tipo de información, datos, voz, imágenes y video. Incluye, infraestructura de cómputo, redes de telecomunicaciones, sistemas, bases de datos, hardware, software, plataformas, aplicaciones, interfaces, páginas de Internet o cualquier otro medio de comunicación electrónica o digital, sus componentes, medios que almacenen información, entre otros.

XVIII. **Unidad de Ciberseguridad:** la unidad encargada de la ciberseguridad en las Autoridades, y

XIX. Vulnerabilidad: la debilidad, error o defecto de cualquier tipo que pueda ser explotada por una amenaza cibernética.

Las definiciones anteriores se entenderán en singular o plural, según corresponda. A falta de definiciones expresas en la presente Ley, se aplicarán de manera supletoria las definiciones previstas en la Ley Federal de Telecomunicaciones y Radiodifusión, y las que se establezcan en las disposiciones que de esta Ley emanen.

Interpretación

Artículo 6. Corresponde a las Autoridades competentes en materia de Ciberseguridad la interpretación de la presente Ley y de las disposiciones que de ésta emanen. Su interpretación estará sujeta al cumplimiento de las finalidades previstas en el artículo segundo de la presente Ley.

TÍTULO SEGUNDO
DE LAS OBLIGACIONES ESTRUCTURALES EN MATERIA DE CIBERSEGURIDAD

Capítulo Único
Observancia general

Artículo 7. Las Autoridades en el Estado deberán cumplir con las obligaciones en materia de ciberseguridad y su incumplimiento acarreará las responsabilidades y sanciones previstas en la presente Ley y demás ordenamientos legales.

Derechos humanos

Artículo 8. En la observancia y cumplimiento de la presente Ley, las Autoridades en el Estado deberán respetar los derechos humanos previstos en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales en los que

el Estado mexicano sea parte y en la Constitución Política del Estado Libre y Soberano de Nuevo León.

Liderazgo

Artículo 9. Los titulares de las Autoridades u órganos de gobierno deberán liderar los esfuerzos necesarios para el cumplimiento de la presente Ley.

Por la obligación de liderazgo se entenderá todos los esfuerzos y gestiones para brindar facilidades y recursos económicos, técnicos y humanos especializados, necesarios y suficientes para cumplir con las finalidades previstas en el artículo segundo de la presente Ley.

Responsabilidad

Artículo 10. Los titulares de las Autoridades y de las Unidades de Ciberseguridad son responsables del cumplimiento de la presente Ley y de las disposiciones que de ésta emanen, en el ámbito de sus atribuciones.

Corresponsabilidad

Artículo 11. Los servidores públicos y prestadores de servicios de las Autoridades tienen la obligación de cumplir con las obligaciones previstas en la presente Ley y con las disposiciones que de ésta emanen.

Confianza digital

Artículo 12. Los titulares de las Autoridades y de las Unidades de Ciberseguridad deben realizar los esfuerzos que sean necesarios para generar, incrementar y fortalecer la confianza digital de los servidores públicos y ciudadanos en los procedimientos, trámites y servicios públicos electrónicos a su cargo.

Neutralidad tecnológica

Artículo 13. No se podrá excluir por disposición legal u orden administrativa una tecnología en particular que sea necesaria para el cumplimiento de la presente Ley, salvo que la misma contravenga su objeto.

Mejores prácticas

Artículo 14. Las Unidades de Ciberseguridad están obligadas a monitorear, identificar, analizar y, en su caso, implementar las mejores prácticas nacionales e internacionales en materia de ciberseguridad que coadyuven en el cumplimiento de la presente Ley.

Gestión de riesgos

Artículo 15. Las Unidades de Ciberseguridad deberán contar con procesos de gestión de riesgos.

Manejo de crisis y resiliencia

Artículo 16. Las Autoridades deberán de contar con protocolos de control de crisis y generar resiliencia en materia de ciberseguridad, incluidos planes de continuidad operativa.

Cultura de ciberseguridad

Artículo 17. Las Autoridades tienen la obligación de capacitar en materia de ciberseguridad, al menos dos veces por año, a todos sus servidores públicos y prestadores de servicios. De igual manera, tienen la obligación de abatir el desconocimiento en materia de ciberseguridad en empresas y ciudadanos, en particular, en niñas, niños y adolescentes.

Ciberseguridad primero

Artículo 18. Todo proyecto, actividad, procedimiento, trámite y servicio de las Autoridades que en todo o en parte haga o pretenda hacer uso de las TIC deberá contar de manera previa con un dictamen de ciberseguridad favorable.

Toda contratación que pretendan realizar las Autoridades de servicios de TIC y de servicios de ciberseguridad deberá contar de manera previa con el dictamen a que se refiere el párrafo anterior.

Proveedores y dependencias tecnológicas

Artículo 19. Las Autoridades deberán determinar sus dependencias tecnológicas y cadena de proveedores tecnológicos a efecto de la identificación de vulnerabilidades directas e indirectas que pongan o puedan poner en riesgo el cumplimiento de las finalidades previstas en el artículo segundo de la presente Ley.

Punto de contacto

Artículo 20. Las Autoridades deberán contar con información de contacto, pública y disponible en todo momento, para la atención de asuntos en materia de ciberseguridad.

Máxima diligencia

Artículo 21. Todos los esfuerzos, acciones y obligaciones a efecto de cumplir con el objeto y finalidades de la presente Ley serán ejecutados por las Autoridades con la máxima diligencia.

Por máxima diligencia deberá entenderse el máximo cuidado, prudencia, agilidad y prontitud.

Ciberseguridad progresiva

Artículo 21. Las Autoridades deberán planear y destinar recursos suficientes y necesarios para el cumplimiento de la presente Ley. El presupuesto anual destinado y aprobado en materia de ciberseguridad por las Autoridades no podrá reducirse.

Evidencia digital

Artículo 23. Las Unidades de Ciberseguridad deberán documentar y configurar los controles en materia de TIC y de ciberseguridad, de tal manera que permitan generar evidencia de acciones u omisiones que, de manera directa o indirecta, dañen, perturben, vulneren, comprometan o pongan en riesgo las finalidades previstas en el artículo segundo de la presente Ley y que permitan constituir indicios o elementos de prueba para el inicio y sustanciación de procedimientos legales de responsabilidad administrativa y penal.

Impacto económico

Artículo 24. Las Autoridades deberán realizar los análisis necesarios a efecto de identificar los impactos económicos directos e indirectos en materia de Ciberseguridad. Los análisis contemplarán, al menos, inversiones, costos directos e indirectos de ataques y, en su caso, estimaciones.

Las Autoridades deberán tomar en consideración los análisis referidos en el párrafo anterior a efecto de cumplir con las finalidades previstas en el artículo segundo de la presente Ley y conducir de manera responsable y sustentada el cumplimiento de esta Ley.

Cooperación institucional

Artículo 25. Las Unidades de Ciberseguridad deberán compartir información entre sí, con la Oficina de Ciberseguridad y con el EIRIC sobre vulnerabilidades, amenazas cibernéticas y ataques, a efecto de prevenirlos, mitigarlos o eliminar sus efectos.

Denuncias por faltas administrativas

Artículo 26. Todos los servidores públicos y prestadores de servicios de las Autoridades deberán denunciar ante la Autoridad Investigadora cualquier acto u omisión del que tengan conocimiento que contravenga lo previsto en la presente Ley.

Procuración de justicia

Artículo 27. Todos los servidores públicos y prestadores de servicios de las Autoridades, en caso de tener conocimiento de hechos que presumiblemente puedan constituir un delito en contra de la ciberseguridad del Estado, deberán presentar denuncia ante la Fiscalía General de Justicia del Estado o Fiscalía especializada en Delitos Cibernéticos.

TÍTULO TERCERO
DE LAS AUTORIDADES EN MATERIA DE CIBERSEGURIDAD
Capítulo I
De la Oficina de Ciberseguridad

Artículo 28. El Estado contará con una Oficina de Ciberseguridad que dependerá de manera directa del titular del Ejecutivo del Estado, quien se encargará del estudio, diseño, análisis, instrumentación, coordinación y promoción de todas las acciones y esfuerzos necesarios en materia de ciberseguridad en el ámbito de las atribuciones que fijan esta Ley y demás disposiciones legales aplicables. En el ejercicio de sus atribuciones, la Oficina de Ciberseguridad estará dotada de autonomía técnica y de gestión para decidir sobre su funcionamiento y actuaciones.

La Oficina de Ciberseguridad contará con un equipo multidisciplinario con especialización técnica, legal y económica en la materia. El reglamento de la oficina establecerá la estructura y demás facultades con las que contará.

El titular de la Oficina de Ciberseguridad y el personal adscrito deberán guiarse por los principios de legalidad, objetividad, imparcialidad, certeza, eficiencia, eficacia, máxima diligencia, transparencia y rendición de cuentas.

Artículo 29. El titular de la Oficina de Ciberseguridad será nombrado y removido libremente por el titular del Ejecutivo del Estado.

Para ser titular de la Oficina de Ciberseguridad se deberán cumplir los requisitos siguientes:

I. Ser ciudadano mexicano, en pleno goce de sus derechos civiles y políticos;

II. Tener cuando menos veintinueve años cumplidos al día de su designación;

III. Gozar de buena reputación y no haber sido condenado por delito doloso que amerite pena de prisión;

IV. Contar con título y cédula profesional expedidos legalmente;

V. Acreditar contar con conocimientos en materia de ciberseguridad y de TIC necesarios para el ejercicio del cargo, y

VI. Contar, al menos, con tres años de experiencia en el servicio público.

Artículo 30. La Oficina de Ciberseguridad tendrá las atribuciones siguientes:

I. Coordinar las acciones y esfuerzos en materia de ciberseguridad en el Estado y celebrar con las Autoridades los instrumentos adecuados para ello;

II. Elaborar la política general de ciberseguridad y modificarla cuando sea necesario;

III. Elaborar políticas sectoriales de ciberseguridad y modificarlas cuando sea necesario;

IV. Crear o modificar mediante acuerdo las áreas administrativas necesarias para su desempeño profesional, eficiente y eficaz, de acuerdo con su presupuesto autorizado;

V. Emitir opinión cuando lo considere pertinente o a solicitud de las Autoridades respecto de proyectos, actos o políticas de las Autoridades en la materia o

relacionadas con las finalidades previstas en el artículo segundo de la presente Ley, sin que esas opiniones tengan efectos vinculantes. Las opiniones deberán publicarse;

VI. Promover una cultura de ciberseguridad en coordinación con las Autoridades;

VII. Asesorar a las Autoridades en la implementación de las políticas en materia de ciberseguridad;

VIII. Asesorar a las Autoridades en recursos humanos, técnicos y financieros en materia de ciberseguridad;

IX. Desarrollar capacidades en las Autoridades en materia de ciberseguridad;

X. Elaborar y publicar el índice de ciberseguridad del Estado;

XI. Elaborar programas de trabajo en materia de ciberseguridad;

XII. Elaborar informes cuatrimestrales de actividades que deberán ser presentados a los Poderes Ejecutivo y Legislativo del Estado;

XIII. Solicitar estudios que evalúen el desempeño de las facultades otorgadas a las Autoridades en materia de ciberseguridad, los cuales serán elaborados por expertos independientes;

XIV. Prestar asistencia y asesoramiento en el diseño y elaboración de leyes y reformas legales relacionadas con las TIC y la ciberseguridad en el Estado;

XV. Sensibilizar a los sectores educativos, empresariales y a la ciudadanía en materia de ciberseguridad;

XVI. Desarrollar, promover y solicitar estudios, trabajos de investigación e informes en materia de ciberseguridad;

XVII. Proponer modificaciones o mejoras a los planes de estudios a las instituciones educativas a efecto de mejorar el conocimiento, cultura y capacidades en materia de ciberseguridad;

XVIII. Compartir información de su competencia con las Autoridades correspondientes;

XIX. Emitir requerimientos de información y documentos relacionados con el ejercicio de sus atribuciones e integrar sus expedientes;

XX. Reiterar los requerimientos de información que formule en aquellos casos donde el desahogo de los mismos resulte insuficiente para tenerlos por desahogados;

XXI. Expedir copias certificadas, certificaciones o cotejos de los documentos existentes en las áreas a su cargo o que le sean presentados;

XXII. Expedir copias certificadas, certificaciones o realizar cotejos de documentos o información para integrarlos a sus expedientes;

XXIII. Emitir oficios de comisión a efecto de llevar a cabo las diligencias necesarias para el cumplimiento de sus atribuciones;

XXIV. Realizar a través de los servidores públicos adscritos las notificaciones de las determinaciones que emita, sin previo acuerdo de comisión;

XXV. Proporcionar la información que le sea requerida por cualquier autoridad administrativa o judicial;

XXVI. Emitir guías, lineamientos y cualquier documento que sea necesario para el cumplimiento de la presente Ley;

XXVII. Convocar a las Autoridades a reuniones y someter a su consideración asuntos de su competencia;

XXVIII. Participar en foros, reuniones, eventos y convenciones en materia de ciberseguridad;

XXIX. Presentar denuncias ante el ministerio público respecto de probables conductas delictivas en contra de la ciberseguridad del Estado de que tenga conocimiento y fungir como coadyuvante;

XXX. Presentar denuncias ante la Autoridad Investigadora por el incumplimiento de la presente Ley y de las disposiciones que de ésta emanen, y fungir como coadyuvante;

XXXI. Tramitar y resolver los asuntos de su competencia, y

XXXII. Las demás que le confieran esta Ley, su reglamento interno y otras disposiciones legales.

Capítulo II

Del Equipo de Inteligencia y Respuesta a Incidentes de Ciberseguridad

Artículo 31. El Estado contará con un EIRIC, que dependerá de manera directa del titular de la Oficina de Ciberseguridad, quien se encargará de la ejecución de las acciones de inteligencia, preventivas y reactivas en materia de ciberseguridad, así como del análisis forense en la materia.

El EIRIC contará con el personal necesario para el cumplimiento de su objeto. En su integración se adoptarán las mejores prácticas nacionales e internacionales.

Artículo 32. El titular del EIRIC será nombrado y removido libremente por el titular de la Oficina de Ciberseguridad.

Para ser titular del EIRIC se deberán cumplir los requisitos siguientes:

I. Ser ciudadano mexicano, en pleno goce de sus derechos civiles y políticos;

II. Tener cuando menos veintinueve años cumplidos al día de su designación;

III. Gozar de buena reputación y no haber sido condenado por delito doloso que amerite pena de prisión;

IV. Contar con título y cédula profesional expedidos legalmente o, al menos, con una certificación vigente en la materia, emitida por entidad reconocida;

V. Acreditar contar con conocimientos técnicos en materia de ciberseguridad y de TIC necesarios para el ejercicio del cargo, y

VI. Acreditar contar, al menos, con cuatro años de experiencia en equipos de respuesta a incidentes de ciberseguridad, centros de operaciones de seguridad o equivalentes.

Artículo 33. El EIRIC cuenta con las atribuciones siguientes:

I. Coadyuvar con la Oficina de Ciberseguridad en el cumplimiento de sus atribuciones previstas en la presente Ley y en las disposiciones de que de ésta emanen;

II. Realizar acciones de inteligencia y monitoreo de amenazas cibernéticas;

III. Analizar, diseñar, implementar y promover acciones preventivas en materia de Ciberseguridad;

IV. Realizar análisis forense que permita iniciar, sustanciar y aportar elementos de prueba en procedimientos de responsabilidad administrativa y penal;

V. Responder de manera inmediata con las herramientas a su alcance a efecto de contener, suprimir o mitigar los efectos de una amenaza cibernética, ataque o cualquier incidente que ponga en riesgo las finalidades previstas en el artículo segundo de la presente Ley;

VI. Dar aviso oportuno a las Autoridades correspondientes de cualquier amenaza cibernética;

VII. Emitir alertas en materia de ciberseguridad;

VIII. Desarrollar capacidades en las Unidades de Ciberseguridad que permitan replicar parte de sus actividades, y

IX. Las demás que le confieran esta Ley y otras disposiciones legales.

Capítulo III
De las Unidades de Ciberseguridad

Artículo 34. Todas las Autoridades contarán con una Unidad de Ciberseguridad, quienes serán las responsables de garantizar su seguridad cibernética y de cumplir con lo previsto en la presente Ley. Los municipios del Estado contarán, al menos, con una Unidad de Ciberseguridad.

Todas las áreas que conformen la estructura orgánica de las Autoridades están obligadas a cooperar con su Unidad de Ciberseguridad.

Artículo 35. El titular de la Unidad de Ciberseguridad de las Autoridades será nombrado y removido libremente por quien tenga facultades para ello.

Artículo 36. Para ser titular de la Unidad de Ciberseguridad se deberán cumplir los requisitos siguientes:

I. Ser ciudadano mexicano, en pleno goce de sus derechos civiles y políticos;

II. Tener cuando menos veintisiete años cumplidos al día de su designación;

III. Gozar de buena reputación y no haber sido condenado por delito doloso que amerite pena de prisión;

IV. Contar con título y cédula profesional expedidos legalmente o con al menos una certificación vigente en la materia, emitida por entidad reconocida;

V. Acreditar contar con conocimientos técnicos en materia de Ciberseguridad y TIC necesarios para el ejercicio del cargo, y

VI. Acreditar contar, al menos, con cuatro años de experiencia en equipos de respuesta a incidentes de ciberseguridad, centros de operaciones de ciberseguridad o equivalentes.

Artículo 37. Las Unidades de Ciberseguridad cuentan con las atribuciones siguientes:

I. Aplicar la política general de ciberseguridad al interior de la Autoridad y, de ser el caso, diseñar e implementar los controles adicionales que considere necesarios;

II. Emitir políticas sectoriales en materia de ciberseguridad;

III. Desarrollar capacidades al interior de las Autoridades en materia de ciberseguridad;

IV. Preparar y recabar la información y documentos necesarios para la elaboración del índice a que se refiere el artículo 45 de la presente Ley;

V. Emitir los dictámenes a que se refiere el artículo 19 de la presente Ley y remitirlos a la Oficina de Ciberseguridad;

VI. Desahogar en tiempo y forma los requerimientos de información emitidos por la Oficina de Ciberseguridad y por el EIRIC;

VII. Emitir guías, lineamientos y cualquier documento que sea necesario para el cumplimiento de la presente Ley;

VIII. Emitir alertas en materia de ciberseguridad;

IX. Realizar con máxima diligencia cualquier acto que sea necesario para cumplir con las finalidades previstas en el artículo segundo de la presente Ley, y

X. Las demás que le confieran esta Ley y otras disposiciones legales.

Artículo 38. Una Unidad de Ciberseguridad podrá ser la responsable del cumplimiento de la presente Ley en dos o más Autoridades, cuando por el tamaño, estructura o presupuesto una Autoridad no pueda contar con su propia unidad.

La asunción de responsabilidad a que se refiere el párrafo anterior deberá formalizarse mediante acuerdo publicado en el Periódico Oficial del Estado, con la anuencia de los titulares de las

Capítulo IV
De la Autoridad Investigadora

Artículo 39. La Autoridad Investigadora verificará, en el ámbito de su competencia, el cumplimiento de la presente Ley.

TÍTULO CUARTO
DE LAS POLÍTICAS EN MATERIA DE CIBERSEGURIDAD
Capítulo I
De la Política General de Ciberseguridad

Artículo 40. El Estado contará con una política general de ciberseguridad, en la cual se establecerán los controles mínimos necesarios a efecto de cumplir con las finalidades previstas en el artículo segundo de la presente Ley.

La Oficina de Ciberseguridad realizará todas las gestiones, acciones y requerimientos necesarios a las Autoridades para la elaboración de la política prevista en el presente artículo.

En la elaboración de la política general de ciberseguridad participarán, al menos, un representante de los Poderes Ejecutivo, Legislativo y Judicial, así como de los órganos constitucionales autónomos. En caso de no lograr un consenso, cada poder y entidad autónoma emitirá su propia política general de ciberseguridad, la cual será obligatoria para todas sus autoridades adscritas.

La política general de ciberseguridad será de observancia obligatoria para todas las Autoridades, sus servidores públicos y prestadores de servicios.

Capítulo II
De las Políticas Sectoriales de Ciberseguridad

Artículo 41. El Estado podrá contar con políticas sectoriales de ciberseguridad, las cuales establecerán obligaciones específicas de acuerdo con las necesidades del sector gubernamental o público que corresponda.

Las Unidades de Ciberseguridad serán las responsables de analizar la pertinencia de emitir políticas sectoriales de Ciberseguridad.

La política sectorial de ciberseguridad será obligatoria para las Autoridades del sector correspondiente.

TÍTULO QUINTO
DEL ÍNDICE, INFORMES Y EJERCICIOS EN MATERIA DE CIBERSEGURIDAD PARA LA MEJORA CONTINUA

Capítulo I
Del Índice de Ciberseguridad

Artículo 42. El Estado contará con un índice que mida y evalúe las capacidades de ciberseguridad de las Autoridades. Las Autoridades están obligadas a tomar en consideración los resultados del índice a efecto de mejorar sus capacidades en materia de seguridad cibernética.

Todas las Autoridades están obligadas a proporcionar la información y documentos necesarios, así como a brindar las facilidades necesarias para la elaboración del índice.

Las Autoridades son responsables de la veracidad de la información proporcionada para la elaboración del índice.

El Índice será publicado en la página de Internet de la Oficina de Ciberseguridad.

Capítulo II
De los informes anuales en materia de Ciberseguridad

Artículo 43. Las Unidades de Ciberseguridad deberán elaborar y rendir un informe anual en materia de Ciberseguridad que será presentado a su titular de la Autoridad y remitirá copia a la Oficina de Ciberseguridad.

La Oficina de Ciberseguridad establecerá los rubros que deberá contener el informe previsto en este artículo y elaborará un reporte con el contenido de los informes que le sean remitidos, el cual presentará a los Poderes Ejecutivo y Legislativo del Estado dentro de los tres primeros meses de cada año.

Artículo 44. La Oficina de Ciberseguridad elaborará y rendirá un informe anual sobre su actuar, que será presentado al titular del Poder Ejecutivo y al Poder Legislativo.

Capítulo III
De los Ejercicios en materia de Ciberseguridad

Artículo 45. Las Autoridades podrán realizar ejercicios controlados en materia de ciberseguridad a efecto de identificar vulnerabilidades y subsanar áreas de oportunidad.

TÍTULO SEXTO
DE LOS PROVEEDORES TECNOLÓGICOS EXTERNOS

Capítulo I
De los Proveedores en materia de Ciberseguridad

Artículo 46. Todos los proveedores de soluciones tecnológicas en materia de Ciberseguridad del Estado deberán acreditar experiencia y contar, al menos, con una certificación vigente en la materia, emitida por una entidad reconocida.

Todo proveedor que no acredite lo establecido en el párrafo anterior no podrá ser contratado por las Autoridades.

Capítulo II

De los Proveedores de TIC

Artículo 47. Todos los proveedores de TIC del Estado deberán acreditar que sus TIC cuentan con controles o especificaciones en materia de Ciberseguridad y, de ser el caso, que cumplen con lo previsto en la Ley Federal de Telecomunicaciones y Radiodifusión.

Todo proveedor que no acredite lo establecido en el párrafo anterior no podrá ser contratado por las Autoridades.

Capítulo III
De las Garantías para el Estado

Artículo 48. Todos los proveedores en materia de Ciberseguridad y de TIC deberán garantizar, según corresponda, que sus productos y servicios contribuirán en el cumplimiento de las finalidades previstas en el artículo segundo de la presente Ley.

Artículo 49. Todo contrato, convenio u equivalente, mediante el cual se formalice la prestación de servicios en materia de ciberseguridad y de TIC deberá establecer sanciones y procedimientos claros en caso de incumplimiento por parte de los proveedores.

Las sanciones serán proporcionales a los daños que se puedan causar.

Todo proveedor que no acepte por escrito el contenido del presente artículo no podrá ser contratado por las Autoridades.

Artículo 50. Todo contrato, convenio u equivalente, mediante el cual se formalice la prestación de servicios en materia de ciberseguridad y de TIC deberá establecer obligaciones a los proveedores de entrega de información y documentos de manera inmediata sobre los servicios prestados, así como sanciones y procedimientos claros en caso de incumplimiento por parte de los proveedores.

Las sanciones serán proporcionales a los daños que se puedan causar.

Todo proveedor que no acepte por escrito la obligación prevista en el presente artículo no podrá ser contratado por las Autoridades.

Artículo 51. De ser aplicable, todo contrato, convenio u equivalente, mediante el cual se formalice la prestación de servicios en materia de ciberseguridad y de TIC deberá establecer obligaciones relativas a respaldo y borrado seguro de información.

Artículo 52. Todas las Autoridades deberán de contar con un listado de sus proveedores en materia de ciberseguridad y de TIC.

TÍTULO SÉPTIMO
DE LA OBLIGACIÓN DE COOPERACIÓN
Capítulo Único

Artículo 53. Todas las Autoridades están obligadas a cooperar con la Oficina de Ciberseguridad, así como a brindar la información, soportes y documentos que sean necesarios y que estén relacionados con el cumplimiento de la presente Ley, en los formatos y plazos establecidos. Los requerimientos de información podrán ser a través de medios electrónicos.

En caso de incumplimiento a la obligación prevista en el párrafo anterior, el titular de la Oficina de Ciberseguridad notificará de manera directa al titular de la Autoridad para el inmediato cumplimiento del requerimiento de información. En caso de que persista el incumplimiento, se dejará constancia de ello y se notificará a la Autoridad Investigadora para el inicio de los procedimientos de ley.

Los incumplimientos previstos en al párrafo anterior, serán públicos en la página electrónica de la Oficina de Ciberseguridad.

TÍTULO OCTAVO
DE LA INFORMACIÓN EN MATERIA DE CIBERSEGURIDAD
Capítulo Único

Artículo 54. La información en materia de Ciberseguridad que ponga en riesgo las finalidades previstas en el artículo segundo de la presente Ley tendrá el carácter de reservada.

b

Las Autoridades en materia de ciberseguridad y personal adscrito estarán sujetos a responsabilidad en los casos de divulgación de la información en su posesión derivado del ejercicio de sus atribuciones.

Artículo 55. La política general de ciberseguridad establecerá los registros de eventos de TIC que serán conservados, su plazo de conservación y demás aspectos relevantes que se consideren necesarios para ello.

TÍTULO NOVENO
DE LA ASISTENCIA Y COOPERACIÓN NACIONAL E INTERNACIONAL
Capítulo Único

Artículo 56. La Oficina de Ciberseguridad podrá solicitar asistencia a entidades nacionales e internacionales a efecto de desarrollar recursos humanos especializados en el Estado en materia de ciberseguridad.

Artículo 57. Las Autoridades de ciberseguridad por sí, o a través de las autoridades competentes, y dentro del marco legal aplicable, podrán cooperar y compartir información con otras autoridades estatales, federales e internacionales en asuntos de ciberseguridad.

TÍTULO DÉCIMO
DE LAS RESPONSABILIDADES EN MATERIA DE CIBERSEGURIDAD
Capítulo Único

Artículo 58. Todo acto u omisión de servidores públicos y prestadores de servicios de las Autoridades que incumpla la presente Ley o tenga por objeto o efecto contravenir o poner en riesgo las finalidades previstas en el artículo segundo de la presente Ley constituirá una falta administrativa grave en términos de la Ley de Responsabilidades Administrativas del Estado de Nuevo León

Las conductas previstas en el presente artículo se investigarán y sancionarán en términos de la legislación prevista en el párrafo anterior, sin perjuicio de las responsabilidades de otra naturaleza a que haya lugar.

Transitorios

Artículo Primero. El presente decreto entrará en vigor al día siguiente a su publicación en el Periódico Oficial del Estado.

Artículo Segundo. En un plazo no mayor a ciento ochenta días hábiles a partir de la entrada en vigor del presente decreto, el titular del Ejecutivo del Estado deberá

realizar las modificaciones correspondientes a su estructura orgánica a efecto de contar con la autoridad de la Oficina de Ciberseguridad que se refiere a la presente Ley y deberá emitir su reglamento interno, el cual deberá incluir al EIRIC.

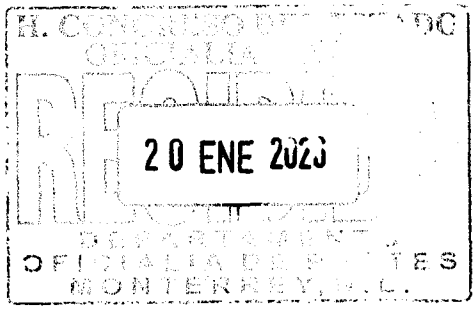
Los recursos materiales y humanos de la Policía Cibernética en el Estado pasarán a formar parte de la Oficina de Ciberseguridad establecida en la presente Ley.

Artículo Tercero. En un plazo no mayor a noventa días hábiles a partir de la entrada en vigor del presente decreto, los titulares de las Autoridades sujetas al presente Decreto deberán realizar las modificaciones correspondientes a sus estructuras orgánicas o equivalentes a efecto de contar con las unidades a que se refiere la presente Ley.

Artículo Cuarto. Se derogan todas aquellas disposiciones legales que se opongan al presente decreto.

Dado en la sede del H. Congreso del Estado Libre y Soberano de Nuevo León, en la Ciudad de Monterrey, al 15 de enero de 2026.

Dip. Sandra Elizabeth Pámanes Ortíz



Dip. Glen Alan Villareal Zambrano

Dip. Ana Melisa Peña Villagomez

Dip. Paola Cristina Linares López

Dip. Marisol González Elías

Dip. Baltazar Gilberto Martínez Ríos **Dip. José Luis Garza Garza**

Dip. Mario Alberto Salinas Treviño **Dip. Armando Víctor Gutiérrez Canales**

Integrantes del Grupo Legislativo de Movimiento Ciudadano
LXXVII Legislatura del H. Congreso del Estado de Nuevo León