

H. Congreso del Estado de Nuevo León



LXXVII Legislatura

PROMOVENTE: DIP. SANDRA ELIZABETH PÁMANEZ ORTIZ, INTEGRANTE DEL GRUPO LEGISLATIVO DE MOVIMIENTO CIUDADANO DE LA LXXVII LEGISLATURA,

ASUNTO RELACIONADO: MEDIANTE EL CUAL PRESENTA INICIATIVA POR LA QUE SE REFORMA LA LEY ORGÁNICA DE LA FISCALÍA GENERAL DE JUSTICIA DEL ESTADO DE NUEVO LEÓN, EN MATERIA DE CIBERSEGURIDAD.

INICIADO EN SESIÓN: 15 DE ENERO DEL 2025

SE TURNÓ A LA (S) COMISION (ES): JUSTICIA Y SEGURIDAD PUBLICA

Mtro. Joel Treviño Chavira

Oficial Mayor



H. CONGRESO DEL ESTADO DE NUEVO LEÓN
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. Rocío Maybe Montalvo Adame, Dip. Paola Cristina Linares López, Dip. Marisol González Elías, Diputados Dip. Miguel Ángel Flores Serna, Dip. Baltazar Gilberto Martínez Ríos, Dip. José Luis Garza Garza, Dip. Armando Victor 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 SE REFORMA LA LEY ORGÁNICA DE LA FISCALÍA GENERAL DE JUSTICIA DEL ESTADO DE NUEVO LEÓN, EN MATERIA DE CIBERSEGURIDAD**, lo que se expresa en la siguiente:

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

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>



Comercio Digital”, en su artículo 19.15, establece un apartado titulado “Ciberseguridad”, en el cual se aprecia lo siguiente:

Lunes 29 de junio de 2020

DIARIO OFICIAL

(Segunda Sección) 441

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, 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 (FISCALÍA 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 anteriormente expuesto, se somete a la consideración de esta Honorable asamblea, el siguiente proyecto de:

DECRETO



ÚNICO. - Se reforma la fracción VII del Artículo 2; se adicionan la fracción VI Bis 2 al Artículo 10; un Capítulo IX BIS denominado “**DE LA FISCALÍA ESPECIALIZADA EN DELITOS CIBERNÉTICOS**” que contiene el artículo 33 bis, a la **Ley Orgánica de la Fiscalía General de Justicia del Estado de Nuevo León**, para quedar como sigue:

ARTÍCULO 2. Para los efectos de esta Ley se entenderá por:

I. a VI. ...

VII. Fiscalías Especializadas: La Fiscalía Especializada en Combate a la Corrupción del Estado de Nuevo León, la Fiscalía Especializada en Delitos Electorales del Estado de Nuevo León; la Fiscalía Especializada Antisecuestros, la Fiscalía Especializada en Feminicidios; la Fiscalía Especializada en Tortura, la Fiscalía Especializada en Inteligencia Financiera, **Fiscalía Especializada en Delitos Cibernéticos** y las demás Fiscalías Especializadas de la Fiscalía General de Justicia del Estado de Nuevo León;

VIII. a X. ...

ARTÍCULO 10. Para el ejercicio de las facultades, funciones y despacho de los asuntos de su competencia, la Fiscalía General se integrará al menos de los siguientes órganos y unidades administrativas:

I. a VI Bis 1. ...

VI Bis 2. Fiscalía Especializada en Delitos Cibernéticos

VII a XVII. ...

...

...



CAPÍTULO IX BIS

DE LA FISCALÍA ESPECIALIZADA EN DELITOS CIBERNÉTICOS

Artículo 33 Ter. La Fiscalía Especializada en Delitos Cibernéticos es la autoridad con capacidades técnicas, encargada de la investigación de hechos que puedan constituir delitos en contra de la ciberseguridad del Estado, en términos de la legislación correspondiente.

La Fiscalía Especializada en Delitos Cibernéticos contará con un equipo multidisciplinario con especialización legal, técnica y económica en la materia. La Ley Orgánica de la Fiscalía General de Justicia del Estado del Estado y su Reglamento establecerá la estructura y atribuciones con las que contará.

TRANSITORIOS.

PRIMERO. - El presente decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial.

SEGUNDO. - La Fiscalía General de Justicia del Estado de Nuevo León tendrá un plazo máximo de 90 días para hacer las modificaciones a su reglamento para el cumplimiento respecto del presente Decreto.

Dado en la sede del H. Congreso del Estado Libre y Soberano de Nuevo León, en la Ciudad de Monterrey, a 09 días del mes de enero de 2025



Dip. Sandra Elizabeth Pámanes Ortiz

Dip. Miguel Ángel Flores Serna



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



Dip. Paola Cristina Linares López

Dip. Ana Melisa Peña Villagomez

Dip. Marisol González Elías

Dip. Rocio Maybe Montalvo Adame

Dip. José Luis Garza Garza

Dip. Baltazar Gilberto Martínez Ríos

Dip. Mario Alberto Salinas Treviño

Dip. Armando Víctor Gutiérrez Canales

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

La presente foja forma parte de la Iniciativa con Proyecto de Decreto por el que se reforma la Ley Orgánica de la Fiscalía General de Justicia del Estado de Nuevo León, de fecha 09 de enero de 2025

