H. Congreso del Estado de Nuevo León

LXXVII Legislatura

PROMOVENTE. C. DIP. JESÚS ALBERTO ELIZONDO SALAZAR, INTEGRANTE DEL GRUPO LEGISLATIVO DE MORENA DE LA LXXVII LEGISLATURA; ASÍ COMO LA C. FRANCISCA ELIZABETH BANDA GARZA, SECRETARIA DE MUJERES DE MORENA

ASUNTO RELACIONADO: PRESENTA INICIATIVA POR LA QUE SE EXPIDE LA LEY DE CIBERPROTECCIÓN PARA NIÑAS, NIÑOS Y ADOLESCENTES PARA EL ESTADO DE NUEVO LEÓN, LA CUAL CONSTA DE 28 ARTÍCULOS Y 4 ARTÍCULOS TRANSITORIOS.

INICIADO EN SESIÓN: 27 DE MAYO DEL 2025

SE TURNÓ A LA (S) COMISION (ES): DE LA FAMILIA Y DERECHOS DE LA PRIMERA INFANCIA, NIÑAS, NIÑOS Y ADOLESCENTES.

Mtro. Joel Treviño Chavira

Oficial Mayor

06

LXXVII
PODER LEGISLATIVO DEL ESTADO DE NUEVO LEON
SEPTUAGÉSIMA SÉPTIMA LEGISLATURA

H. CONGRESO DEL ESTADO
OFICIALIA MAYOR
RECIBIDO
30 ABR 2025
11:13 hrs
DEPARTAMENTO
OFICIALIA DE PARTES
MONTERREY, N.L.

GRUPO LEGISLATIVO
morena

DIP. LORENA DE LA GARZA VENECIA
PRESIDENTA DEL H. CONGRESO DEL ESTADO DE NUEVO LEÓN
PRESENTE. –

Los suscritos diputados **CC. Mario Alberto Soto Esquer, Jesús Alberto Elizondo Salazar** y diputadas **CC. Grecia Benavides Flores** y **Brenda Velázquez Valdez**, a la LXXVII Legislatura del H. Congreso del Estado de Nuevo León, del Grupo Legislativo de Morena, y las **CC. Anabel del Roble Alcocer Cruz, Liliana Solís Barrera y Francisca Elizabeth Banda Garza**, 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, ocurro a promover Iniciativa con Proyecto de Decreto por el que se expide la **Ley de Ciberprotección de Niñas, Niños y Adolescentes para el *Estado de Nuevo León***, con base en la siguiente:

EXPOSICIÓN DE MOTIVOS

La era digital ha transformado la manera en que niñas, niños y adolescentes interactúan, aprenden, se comunican y se desarrollan. Si bien las tecnologías de la información y comunicación (TIC) ofrecen innumerables oportunidades, también presentan riesgos significativos para este grupo etario, particularmente en contextos como el acoso cibernético, la violencia digital, la exposición a contenido inapropiado, el grooming, la explotación sexual en línea y el uso excesivo o adictivo de dispositivos.

En este contexto, el marco jurídico estatal aún presenta vacíos sustanciales respecto a la regulación específica de la ciberprotección de la niñez y adolescencia,

a pesar del incremento exponencial en el uso de dispositivos conectados y redes sociales desde edades cada vez más tempranas.
De acuerdo con el estudio más reciente de UNICEF México (2023), el 87% de niñas, niños y adolescentes entre 10 y 17 años utilizan internet, y uno de cada cinco ha sufrido acoso o violencia digital. Asimismo, el informe "MIND 2023" del Instituto Federal de Telecomunicaciones (IFT) señala que el 63% de usuarios entre 7 y 17 años accede a internet sin supervisión adulta.

Por su parte, la organización Te Protejo México reportó un aumento del 230% en denuncias por abuso sexual digital infantil entre 2020 y 2022. En Nuevo León, datos de la Fiscalía General de Justicia revelan que los delitos contra menores relacionados con tecnologías aumentaron en un 74% desde 2019, particularmente en zonas urbanas como Monterrey, Guadalupe y San Nicolás.

México es Estado parte de la ***Convención sobre los Derechos del Niño*** y ha incorporado en su legislación interna el principio del interés superior de la niñez (Art. 4° Constitucional), así como el derecho a la intimidad, seguridad e integridad personal. Además, la Ley General de Derechos de Niñas, Niños y Adolescentes establece en su Artículo 13 la obligación de garantizar su protección frente a todo tipo de violencia, incluidos los entornos digitales.

Sin embargo, el marco local en Nuevo León carece de una legislación autónoma y especializada que regule la ciberprotección infantil de forma integral, articulada y preventiva. En consecuencia, es necesario armonizar y complementar la legislación estatal para hacer frente a los riesgos emergentes del entorno digital.

Como se ha venido mencionando, la actual legislación de Nuevo León presenta vacíos normativos relevantes, los cuales nos permitimos señalar.

Empezando por la ausencia de una ley sectorial específica. Si bien existen disposiciones dispersas en leyes como la Ley de los Derechos de Niñas, Niños y Adolescentes del Estado de Nuevo León y la Ley de Educación, estas son insuficientes para abordar de manera integral y especializada los nuevos retos que plantea el ecosistema digital. ***No existe una ley que aborde con enfoque de niñez la prevención, protección, participación, denuncia, sanción y reparación vinculadas con entornos virtuales.***

Continuando con la ***falta de mecanismos claros de denuncia y respuesta en casos de violencia digital***. Actualmente no hay una arquitectura normativa que obligue a las autoridades estatales y municipales a implementar canales accesibles, confidenciales, especializados y con tiempos definidos para atender denuncias de violencia o delitos digitales contra personas menores de edad.

Aunado a la ***inexistencia de deberes específicos para plataformas digitales y prestadores de servicios tecnológicos***. La legislación estatal no establece obligaciones mínimas para que los actores privados garanticen espacios digitales seguros, mecanismos de verificación de edad, filtros parentales o protocolos de actuación en casos de difusión de contenido violento o sexual contra menores.

Siguiendo con la ***débil articulación institucional***. La actual fragmentación de competencias entre dependencias educativas, de seguridad, salud, derechos humanos y protección infantil impide respuestas coordinadas ante las amenazas digitales. Se requiere un marco normativo que establezca ***protocolos conjuntos y líneas claras de corresponsabilidad.***

Además tenemos un claro ***vacío en la construcción de ciudadanía digital desde la infancia***. No se reconoce el derecho de niñas, niños y adolescentes a la

alfabetización digital crítica, es decir, a desarrollar habilidades para usar las tecnologías de manera informada, ética, segura y participativa. La educación digital sigue siendo limitada y sin enfoque de derechos.

Así mismo, existe una ***insuficiencia de principios rectores en entornos digitales***. Aunque la legislación local reconoce el interés superior de la niñez, no lo articula con los principios de no discriminación, protección integral, progresividad o participación infantil aplicados específicamente a entornos digitales.

Por todo lo anterior, resulta imperativo expedir una ley estatal especializada, que garantice a niñas, niños y adolescentes de Nuevo León el ejercicio pleno de sus derechos en espacios digitales, que establezca obligaciones para el sector público y privado, articule mecanismos efectivos de prevención, protección y sanción, y promueva una cultura digital incluyente, crítica, segura y participativa desde la infancia.

Así, la presente ley tiene como finalidad garantizar el ejercicio pleno de los derechos digitales de niñas, niños y adolescentes, mediante mecanismos integrales de prevención, detección, atención y sanción de riesgos digitales, con la participación corresponsable de autoridades, familias, instituciones educativas, proveedores de servicios digitales y la sociedad civil.

Esta Ley de Ciberprotección ***no duplica marcos legales existentes***; por el contrario, los fortalece y complementa, dotando de herramientas concretas y contemporáneas al sistema estatal de protección de derechos de niñas, niños y adolescentes, conforme a los más altos estándares nacionales e internacionales en la materia, como la Observación General No. 25 del Comité de los Derechos del Niño de la ONU (2021), sobre los derechos de la infancia en el entorno digital.

Derecho comparado nacional

Ya existen antecedentes relevantes en otras entidades federativas:

- Ciudad de México: Ley de Protección Integral de los Derechos de Niñas, Niños y Adolescentes, con capítulo sobre derechos digitales.
- Jalisco: Protocolo estatal de prevención del acoso cibernético infantil, bajo el marco del Sistema DIF.
- Estado de México: Estrategia de Escuelas Seguras en Línea, incorporada como política pública transversal en el sector educativo.

Derecho comparado internacional

- España (Ley Orgánica para la protección de las personas menores de edad en los entornos digitales 1/2021): Reconoce el derecho a la protección digital de los menores y establece obligaciones específicas para plataformas tecnológicas.
- Colombia: Ley 1620/2013 y Decreto 1965/2013, que regulan la convivencia escolar incluyendo la prevención del ciberacoso.
- Chile: Ley 21.325, que incorpora medidas de protección digital para menores en el contexto escolar y familiar.

Ahora bien, en el capítulo denominado "Riesgos Digitales", se plantean tres términos anglosajones que a manera de precisión y con base a criterios de técnica legislativa, nos permitimos señalar la ***sustituibilidad lingüística*** que permite el uso de términos extranjeros únicamente cuando no exista una palabra equivalente en español o cuando el término sea ténico especializado de uso generalizado en la materia. En tales casos, se recomienda incluir una glosa o nota aclaratoria que explique el significado del término, por lo que describimos dichos términos en la glosa que forma parte de esta Ley, a continuación se mencionan algunos ejemplos del uso de términos anglosajones en la legislación de diversos estados:

1. Código Civil para el Estado de Nuevo León
El artículo 21 Bis III establece que las remisiones a un Derecho extranjero incluyen también las disposiciones remisorias contenidas en el mismo, a menos que sean incompatibles con la finalidad de las remisiones establecidas en el derecho local. Esto reconoce la posibilidad de incorporar términos y conceptos extranjeros en la legislación estatal cuando sea necesario.

2. Manual de Redacción y Estilo del Poder Judicial del Estado de Nuevo León
Este manual establece que las palabras extranjeras deben escribirse en cursiva para señalar su uso metalingüístico o cuando se citan ejemplos dentro del texto. Esto proporciona una guía clara sobre cómo incorporar términos extranjeros en documentos oficiales.

3. Código Penal de la Ciudad de México
Art. 179 Quáter:
"Comete el delito de grooming, quien a través de medios informáticos, de comunicación electrónica..."

Este es un precedente clave para argumentar su constitucionalidad y aceptación técnica.

Justificación técnica y jurídica del uso de términos en inglés en legislación estatal mexicana

1. *Términos sin traducción exacta o con pérdida de precisión*
Cuando el término extranjero describe fenómenos tecnológicos, jurídicos o sociales emergentes que no tienen una traducción exacta al español o cuya traducción

pierde especificidad técnica, puede justificarse su inclusión tal cual, con su correspondiente explicación.

Ejemplo:

- Grooming: no tiene una traducción legal precisa. El equivalente más cercano sería "acoso sexual digital infantil", pero no abarca toda la conducta típica.
- Doxing: tampoco se traduce con claridad. "Divulgación maliciosa de datos personales" es una aproximación, pero no captura la carga del término original.
- Sextorsion: en español se podría traducir como "extorsión sexual digital", pero se justifica el uso del término anglosajón por su empleo extendido en tratados y literatura internacional.

2. *Uso reconocido por organismos internacionales y derecho comparado*

Estos términos se utilizan de manera habitual en instrumentos internacionales, como: Convención de Budapest sobre ciberdelincuencia, resoluciones de la ONU y UNICEF sobre violencia digital, en las guías de INTERPOL y EUROPOL y en la legislación de países como España, Chile, Colombia y Estados Unidos.

Esto permite el uso contextual del término en inglés, especialmente si se acompaña de una definición normativa dentro del propio texto legal.

3. *Reconocimiento en jurisprudencia, doctrina y guías nacionales*

1. El INE, el CONAVIM, el Instituto de Justicia Alternativa del Estado de Jalisco y varias fiscalías estatales han utilizado estos términos en manuales, protocolos y estrategias de prevención.

2. La SCJN y los tribunales colegiados han aceptado en criterios indirectos el uso de extranjerismos cuando se trata de figuras delictivas globales.
3. La Guía de técnica legislativa del Congreso de la Unión permite términos en otros idiomas si se incluyen glosados y definidos en el articulado.

A manera de conclusión, es menester señalar que, la expedición de esta ley responde al urgente llamado de organismos internacionales, expertos, educadores y familias para brindar un entorno digital más seguro a la niñez y adolescencia en Nuevo León. Se trata de garantizar no solo su acceso a la tecnología, sino su desarrollo sano y seguro en la era digital, en estricto apego al principio del interés superior del menor.

Con ello, el Estado de Nuevo León se colocaría como entidad pionera a nivel nacional en legislar de manera integral sobre ciberprotección infantil, alineándose a estándares internacionales y consolidando una política pública preventiva y de largo alcance.

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

DECRETO

PRIMERO.- Se expide la Ley Ciberprotección para Niñas, Niños y Adolescentes para el Estado de Nuevo León, para quedar como sigue:

LEY DE CIBERPROTECCIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES PARA EL ESTADO DE NUEVO LEÓN

TÍTULO PRIMERO
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO Y PRINCIPIOS

Artículo 1. La presente Ley es de orden público, interés social y observancia general en el Estado de Nuevo León. Tiene por objeto establecer las bases, principios y mecanismos para prevenir, detectar, atender y sancionar los riesgos digitales que afecten a niñas, niños y adolescentes.

Artículo 2. La presente Ley tiene como objetivos;

I. Garantizar la protección integral de niñas, niños y adolescentes frente a riesgos, amenazas y violencias que se presenten en el entorno digital;

II. Promover el uso seguro, informado, responsable y ético de las tecnologías de la información y comunicación entre niñas, niños y adolescentes;

III. Establecer mecanismos de prevención, detección, atención y sanción de conductas que vulneren los derechos de niñas, niños y adolescentes en medios digitales;

IV. Fomentar la alfabetización digital crítica, el desarrollo de habilidades digitales y la resiliencia frente a contenidos nocivos o riesgosos;

V. Impulsar la participación activa de niñas, niños y adolescentes en la creación de políticas públicas digitales que garanticen su seguridad y bienestar;

VI. Fortalecer las capacidades institucionales y la coordinación interinstitucional para la protección de niñas, niños y adolescentes en entornos digitales; y

VII. Regular la corresponsabilidad de padres, madres, tutores, prestadores de servicios digitales, instituciones educativas y autoridades en la protección digital infantil.

Artículo 3. Son principios rectores de esta Ley:

I. Interés superior de la niñez;

II. Corresponsabilidad;

III.- Enfoque de derechos;

IV. Protección integral;

V. Participación infantil;

VI. No discriminación; y

VII. Progresividad.

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

I. Autoridades estatales y municipales;

II. Instituciones educativas públicas y privadas;

III. Padres, madres y tutores;

IV. Proveedores de servicios digitales y plataformas tecnológicas; y

V. Organizaciones de la sociedad civil.

Artículo 5. Para los efectos de la presente Ley se entederá por:

I. Alfabetización digital crítica: Desarrollo de habilidades técnicas, cognitivas y éticas para comprender, analizar y usar responsablemente las tecnologías de la información;

II. Ciberacoso: Toda conducta sistemática ejercida mediante medios digitales que cause daño emocional, psicológico o moral a una niña, niño o adolescente;

III. Ciberdelito: Conducta tipificada como delito en el ordenamiento jurídico penal y cometida a través de medios digitales contra niñas, niños o adolescentes;

IV. Contenido nocivo: Cualquier material digital que, por su naturaleza, pueda afectar el desarrollo físico, psicológico, emocional o moral de niñas, niños y adolescentes;

V. Corresponsabilidad: Reconocimiento de la obligación compartida entre Estado, familia, sociedad civil, sector privado y los propios menores en la protección de sus derechos en entornos digitales;

VI. Doxing: Acción consistente en investigar, obtener y divulgar de forma ilícita datos personales, sensibles o de localización de una persona, con el propósito de intimidarla, acosarla o ponerla en riesgo a través de medios digitales;

VII. Enfoque de derechos: Perspectiva que considera a niñas, niños y adolescentes como sujetos plenos de derechos, con capacidad progresiva de ejercerlos, incluso en el ámbito digital;

VIII. Entorno digital: Espacio compuesto por tecnologías de la información, plataformas digitales, redes sociales, aplicaciones móviles y cualquier otro medio digital en el que interactúan niñas, niños y adolescentes;

IX. Grooming: Es la acción deliberada de una persona adulta, realizada por medios digitales, consistente en contactar a una niña, niño o adolescente para establecer una relación de confianza, con el propósito de obtener material sexual o meter actos sexuales en su contra;

X. Interés superior de la niñez: Principio que establece que todas las decisiones, acciones y políticas que afecten a niñas, niños y adolescentes deben priorizar su bienestar integral y desarrollo pleno en el entorno digital;

XI. Ley: Ley de Ciberprotección de niñas, niños y adolescentes para el Estado de Nuevo León y sus Municipios;

XII. No discriminación: Garantía de igualdad, en el acceso, uso y disfrute seguro de las tecnologías, sin distinción por razón de género, edad, discapacidad, origen étnico, situación económica u otra condición;

XIII. Política de Inclusión Digital Universal: Es el conjunto de acciones, programas, normas y estrategias implementadas por el Estado, en coordinación con los sectores público, privado, académico y social, para garantizar que todas las personas, especialmente niñas, niños y adolescentes, tengan acceso equitativo,

asequible, seguro y significativo a las tecnologías de la información y la comunicación (TIC), sin discriminación alguna por razones socioeconómicas, geográficas, culturales, de género, discapacidad o cualquier otra condición;

XIV. Privacidad digital: Derecho de niñas, niños y adolescentes a controlar el acceso, uso y difusión de su información personal en entornos digitales;

XV. Progresividad. Los derechos digitales de niñas, niños y adolescentes deberán expandirse progresivamente, sin retrocesos, ampliando el acceso seguro y responsable a las tecnologías;

XVI. Protección integral: Conjunto de políticas, estrategias y acciones que garantizan el ejercicio, respeto, protección y restitución de derechos de niñas, niños y adolescentes en todos los ámbitos, incluidos los digitales;

XVII. Proveedor de servicios digitales y plataformas tecnológicas: Persona física o moral, pública o privada, que desarrolla, opera, administra o facilita el acceso a plataformas, aplicaciones, redes sociales, sitios web o cualquier otro entorno digital en el que interactúan niñas, niños y adolescentes;

XVIII. Sextorsión: Es un tipo de extorsión sexual en que la persona que sufre el chantaje, generalmente por aplicaciones de mensajería instantánea o redes sociales, es amenazada con una o varias imágenes de sí misma (fotografías o videos) desnuda o realizando actos sexuales.

XIX. Tecnologías de la información y la comunicación (TIC): Conjunto de herramientas, recursos, equipos, programas, sistemas y redes que permiten el acceso, generación, almacenamiento, procesamiento, transmisión, intercambio y gestión de información y contenidos digitales, mediante dispositivos electrónicos como computadoras, teléfonos inteligentes, tabletas, plataformas digitales, aplicaciones móviles, redes sociales, internet y demás medios tecnológicos relacionados; y

XX. Violencia digital: Actos que causan daño psicológico, moral, sexual o económico a través de medios tecnológicos, redes sociales o plataformas en línea.

TÍTULO SEGUNDO
DERECHOS DIGITALES Y RIESGOS CIBERNÉTICOS

CAPÍTULO I
DERECHOS DIGITALES DE NIÑAS, NIÑOS Y ADOLESCENTES

Artículo 6. Toda niña, niño y adolescente goza del derecho de acceso universal a las Tecnologías de la Información y Comunicación (TIC), así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet.

Artículo 7. Toda niña, niño y adolescente tiene derecho a:
I. Acceder de forma segura a las tecnologías digitales;
II. Recibir educación digital crítica y responsable;
III. Ser protegido frente a contenidos nocivos o delictivos;
IV. La privacidad y confidencialidad de su información; y
V. Participar en la formulación de políticas digitales.

Artículo 8. Las autoridades garantizarán a niñas, niños y adolescentes su integración a la sociedad de la información y el conocimiento e impulsarán el uso de las tecnologías de la información y la comunicación mediante una política de inclusión digital universal en condiciones de equidad, asequibilidad, disponibilidad, accesibilidad, calidad. El reglamento y las reglas de operación determinarán los criterios para establecer las acciones y la progresividad de este derecho.

Artículo 9. Toda niña, niño y adolescente tiene derecho al acceso y uso seguro del Internet como medio efectivo para ejercer los derechos a la información, comunicación, educación, salud, esparcimiento, no discriminación, de conformidad con el principio de interdependencia, en términos de las disposiciones aplicables. Asimismo, tendrán derecho a recibir información suficiente y necesaria sobre el uso responsable, respetuoso y adecuado de las tecnologías.

CAPÍTULO II

RIESGOS DIGITALES

Artículo 10. Se consideran riesgos digitales:

I. Ciberacoso o bullying digital;

II. Grooming;

III. Sextorsión;

IV. Exposición a contenido sexual explícito;

V. Retos virales peligrosos;

VI. Adicción a dispositivos electrónicos; y

VII. Doxing (difusión de datos personales sin consentimiento).

TÍTULO TERCERO
SISTEMA ESTATAL DE CIBERPROTECCIÓN

CAPÍTULO I
INTEGRACIÓN Y FUNCIONES

Artículo 11. Se crea el Sistema Estatal de Ciberprotección de Niñas, Niños y Adolescentes, encabezado por el DIF estatal, e integrado por:

I. Secretaría de Educación;

II. Fiscalía General del Estado;

III. Policía Cibernética;

IV. Comisión Estatal de Derechos Humanos;

V. Sociedad civil; y

VI. Plataforma digital de denuncia anónima.

Artículo 12. El Sistema deberá:

I. Diseñar políticas públicas de prevención;

II. Establecer protocolos de actuación;

III. Promover campañas informativas; y

IV. Coordinar acciones de protección y sanción.

TÍTULO CUARTO
PREVENCIÓN, DENUNCIA Y SANCIÓN

CAPÍTULO I
EDUCACIÓN Y PREVENCIÓN

Artículo 13. La Secretaría de Educación deberá incorporar contenidos de alfabetización digital crítica en todos los niveles escolares.

Artículo 14. Las instituciones educativas deberán implementar protocolos internos ante casos de violencia digital.

Artículo 15. Actividades de formación en las escuelas públicas y privadas.

La Secretaría de Educación fomentará en la educación básica, el desarrollo de actividades encaminadas a la mejora de la competencia digital con el fin de garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro, saludable, sostenible, crítico y responsable de las tecnologías de la información y la comunicación para el aprendizaje, el trabajo y la participación en la sociedad, así como la interacción con estas.

Además deberán incluir en su planificación de la formación continua del personal docente, actividades formativas que faciliten a los docentes estrategias para incidir, entre otros aspectos, en la seguridad (incluido el bienestar digital y las competencias

relacionadas con la ciberseguridad) y en asuntos relacionados con las tecnologías de la información y la comunicación.

Artículo 16. Regulación del uso de dispositivos en escuelas.
Las escuelas de primaria y secundaria regularán el uso de dispositivos móviles y digitales en las aulas, en las actividades extraescolares y en lugares y tiempos de descanso que tengan lugar bajo su supervisión.

CAPÍTULO II
MECANISMOS DE DENUNCIA

Artículo 17. De los canales de denuncia:
El Estado garantizará la existencia de canales accesibles, seguros, confidenciales y eficaces para que niñas, niños, adolescentes, sus madres, padres, tutores o cualquier persona puedan denunciar hechos que vulneren los derechos de personas menores de edad en entornos digitales.

Dichos canales deberán estar disponibles en línea, por vía telefónica y de manera presencial, funcionando de forma ininterrumpida y con enfoque especializado.

Artículo 18. Toda niña, niño o adolescente podrá denunciar hechos de violencia digital a través de:
I. Plataformas electrónicas del Sistema Estatal;
II. Instituciones educativas;
III. Línea directa de protección; y
IV. Fiscalía especializada.

Artículo 19. Del procedimiento de atención:
Las denuncias recibidas deberán ser atendidas de forma inmediata por las autoridades competentes, quienes activarán un protocolo de actuación con perspectiva de niñez.
Este incluirá la evaluación del riesgo, la implementación de medidas de protección urgentes, la salvaguarda de la integridad de la niña, niño o adolescente, y su canalización a servicios de atención médica, psicológica, jurídica o social.

Artículo 20. Del anonimato y la confidencialidad:
Toda denuncia podrá presentarse de manera anónima. Las autoridades deberán garantizar en todo momento la confidencialidad de la identidad de la persona denunciante, así como de la víctima, especialmente si se trata de niñas, niños o adolescentes.
El manejo de la información deberá observar estrictamente lo dispuesto en la legislación en materia de protección de datos personales.

Artículo 21. De la coordinación interinstitucional:
Las autoridades en materia de derechos de niñas, niños y adolescentes, procuración de justicia, seguridad pública, educación, salud y tecnologías de la información establecerán mecanismos permanentes de coordinación interinstitucional para la recepción, seguimiento y resolución de denuncias sobre riesgos digitales.

Deberán celebrarse convenios de colaboración para el intercambio de información, atención especializada y prevención integral.

Artículo 22. Del registro de denuncias y estadísticas:

Se integrará un Registro Estatal de Denuncias por Riesgos Digitales contra Niñas, Niños y Adolescentes, bajo la rectoría de la Procuraduría de Protección de Niñas, Niños y Adolescentes.

Este registro tendrá fines estadísticos y de formulación de políticas públicas, con información desagregada por tipo de riesgo, edad, sexo, localidad, medio digital utilizado y estado de resolución.

El tratamiento de los datos deberá garantizar en todo momento la confidencialidad e interés superior de la niñez.

CAPÍTULO III
SANCIONES

Artículo 23. De los sujetos responsables.

Serán sujetos de responsabilidad administrativa, civil o penal conforme a esta Ley, sin perjuicio de otras disposiciones aplicables:

I. Las madres, padres o tutores que incumplan sus deberes de supervisión digital cuando con ello expongan a las niñas, niños o adolescentes a riesgos previsibles o reiterados;

II. Las autoridades educativas, de salud, seguridad o protección de derechos que omitan, nieguen o retrasen injustificadamente la atención a denuncias o reportes sobre violencia digital en contra de personas menores de edad;

III. Los proveedores de servicios digitales y plataformas tecnológicas que no adopten medidas mínimas de prevención, monitoreo, reporte y remoción de contenidos nocivos dirigidos a niñas, niños o adolescentes; y

IV. Las instituciones públicas o privadas que difundan, promuevan, almacenen o toleren la circulación de material digital que constituya violencia, acoso, explotación o discriminación infantil.

Artículo 24. De las sanciones administrativas

La autoridad competente podrá imponer, según la gravedad de la falta y la reincidencia:

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 penal o administrativa conforme a otras leyes aplicables.

Artículo 25. De las sanciones penales y civiles

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.

Artículo 26. De las omisiones graves

Se considerarán omisiones graves, y darán lugar a responsabilidad directa:

I. Negarse a recibir denuncias o no activar los protocolos de protección establecidos, tratándose de niñas, niños o adolescentes expuestos a violencia digital;

II. No retirar o bloquear contenidos nocivos o ilegales en un plazo razonable, cuando exista requerimiento de autoridad competente o evidencia clara del daño;

III. Repetir omisiones previamente sancionadas en materia de protección digital infantil;

IV. Minimizar, invisibilizar o responsabilizar a la víctima por hechos de violencia digital; y

V. No implementar mecanismos de control parental, verificación de edad o filtros de contenido en plataformas dirigidas o accesibles a menores.

Artículo 27. De los atenuantes y agravantes

Para determinar la sanción, se considerarán como atenuantes: la colaboración activa con la autoridad, reparación del daño, medidas de no repetición y cumplimiento espontáneo.

Y como agravantes: reincidencia, daño psicológico severo, afectación a múltiples víctimas, difusión masiva o viral del contenido nocivo, y participación de servidores públicos.

Artículo 28. De las autoridades competentes para sancionar

La Procuraduría de Protección de Niñas, Niños y Adolescentes, la Secretaría de Educación, la Comisión Estatal de Derechos Humanos y otras autoridades administrativas competentes podrán imponer las sanciones previstas en este capítulo, sin perjuicio de la intervención de órganos jurisdiccionales.

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 Ciberprotección deberá integrarse en un plazo máximo de 90 días a partir de la entrada en vigor del presente Decreto.

ARTÍCULO CUARTO.- 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.

Atentamente

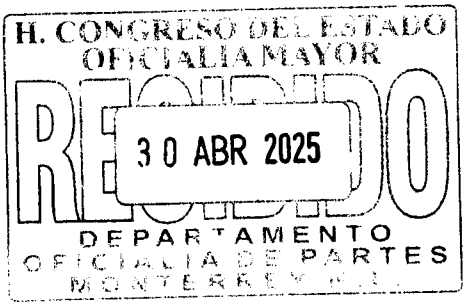
Monterrey, Nuevo León a 30 de abril del 2025

DIPUTADO MARIO ALEJANDRO SOTO ESQUER
COORDINADOR DE LA BANCADA DE MORENA

DIPUTADO JESÚS ALBERTO ELIZONDO SALAZAR

DIPUTADO BRENDA VELÁZQUEZ VALDEZ

DIPUTADA GRECIA BENAVIDES FLORES



LXXVII
PODER LEGISLATIVO DEL ESTADO DE NUEVO LEÓN
SEPTUAGÉSIMA SÉPTIMA LEGISLATURA

GRUPO LEGISLATIVO
morena

INTEGRANTES DEL COMITÉ EJECUTIVO ESTATAL

ANABEL DEL ROBLE ALCOCER CRUZ
PRESIDENTA

LILIANA SOLÍS BARRERA
SECRETARIA DE COMUNICACIÓN

[redacted]

FRANCISCA ELIZABETH BANDA GARZA
SECRETARIA DE MUJERES

H. CONGRESO DEL ESTADO
OFICIALIA MAYOR
RECIBIDO
30 ABR 2025
11:13
DEPARTAMENTO
OFICIALIA DE PARTES
MONTERREY N.L.