

Proyecto de Ley

La Honorable Cámara de Diputados de la Nación y el Senado...

SANCIONAN:

SISTEMA NACIONAL DE CERTIFICACIÓN "ESPACIO SEGURO DIGITAL"

CAPÍTULO I: DISPOSICIONES GENERALES

Artículo 1º — Objeto

Créase el Sistema Nacional de Certificación "Espacio Seguro Digital", destinado a reconocer a las instituciones educativas, deportivas, recreativas, culturales y formativas que desarrollen actividades con niñas, niños y adolescentes y que acrediten el cumplimiento de estándares de seguridad de su infraestructura digital, protección de la privacidad, seguridad de sus redes y dispositivos institucionales y capacitación del personal responsable de su administración y uso.

El Sistema tendrá por finalidad promover la adopción de medidas técnicas y organizativas que permitan reducir la exposición a contenidos inapropiados y amenazas informáticas, fortalecer la protección de los datos personales y mejorar las condiciones de seguridad de los entornos digitales bajo responsabilidad de las instituciones.

Artículo 2º — Ámbito de aplicación

Podrán solicitar el "Sello Espacio Seguro Digital":

- a) establecimientos educativos de gestión estatal y privada;
- b) clubes, asociaciones y entidades deportivas;
- c) instituciones recreativas, culturales, comunitarias o formativas que desarrollen actividades destinadas a niñas, niños y adolescentes.

La certificación comprenderá exclusivamente las condiciones de seguridad digital, infraestructura tecnológica y prácticas institucionales que se encuentren bajo responsabilidad o control de la institución.

La reglamentación establecerá requisitos diferenciados de acuerdo con las características, tamaño, infraestructura, cantidad de usuarios y nivel de riesgo de cada institución.

Artículo 3° — Carácter voluntario

La adhesión al Sistema será voluntaria y no sustituirá las obligaciones establecidas por la legislación vigente en materia de protección integral de niñas, niños y adolescentes, educación, protección de datos personales y ciberseguridad.

CAPÍTULO II: SELLO “ESPACIO SEGURO DIGITAL”

Artículo 4° — Creación

Créase el “Sello Espacio Seguro Digital”, como certificación oficial destinada a identificar a las instituciones que acrediten el cumplimiento de los estándares establecidos por la presente ley y su reglamentación.

Artículo 5° — Requisitos

Para obtener el “Sello Espacio Seguro Digital”, las instituciones deberán acreditar, como mínimo:

- a) La implementación de mecanismos adecuados de seguridad y filtrado en las redes institucionales que proporcionen acceso a Internet;
- b) La adopción de medidas destinadas a restringir el acceso, desde las redes institucionales destinadas a niñas, niños y adolescentes, a contenidos incompatibles con su edad, incluyendo contenidos pornográficos, material de abuso sexual infantil, sitios de apuestas y otras categorías que determine la reglamentación;
- c) La implementación de medidas razonables de protección frente a malware, phishing, sitios maliciosos y otras amenazas informáticas;

- d) La adopción de políticas y procedimientos adecuados para la protección de datos personales y la privacidad;
- e) La existencia de procedimientos institucionales para la detección, gestión y comunicación de incidentes de seguridad digital;
- f) La capacitación periódica del personal que tenga responsabilidades vinculadas con la administración de redes, dispositivos, sistemas o información institucional;
- g) La designación de un responsable institucional de seguridad digital, de acuerdo con las características y dimensiones de la institución.

Los requisitos establecidos deberán aplicarse de manera proporcional a las características y recursos de cada institución.

Artículo 6° — Redes institucionales

Las instituciones que proporcionen acceso a Internet a niñas, niños y adolescentes deberán implementar medidas adecuadas para garantizar la seguridad de sus redes inalámbricas y demás sistemas de conectividad institucional.

Cuando resulte necesario de acuerdo con las características de la institución y el nivel de riesgo identificado, deberán establecerse mecanismos de segmentación entre las redes destinadas a niñas, niños y adolescentes, personal, administración, dispositivos institucionales y visitantes.

Las redes destinadas al acceso de niñas, niños y adolescentes deberán contar con mecanismos adecuados de filtrado y control de contenidos.

La reglamentación establecerá los estándares técnicos mínimos aplicables, incluyendo, según corresponda, mecanismos de filtrado, protección contra sitios maliciosos, gestión de accesos, segmentación de redes, actualización de sistemas y demás medidas necesarias.

Los estándares deberán respetar el principio de neutralidad tecnológica, sin imponer una determinada marca, proveedor, software o solución tecnológica.

Artículo 7° — Privacidad y Protección de Datos

La implementación de mecanismos de seguridad, filtrado y auditoría deberá respetar la legislación vigente en materia de protección de datos personales y los principios de finalidad, proporcionalidad, minimización y seguridad.

Las instituciones podrán conservar registros técnicos de conexión únicamente cuando resulten necesarios y proporcionales para fines de seguridad, prevención, investigación y gestión de incidentes.

Dichos registros deberán encontrarse sujetos a medidas adecuadas de seguridad y acceso restringido y conservarse durante el tiempo estrictamente necesario para la finalidad que motivó su obtención.

Queda prohibida la utilización de registros técnicos para fines comerciales, publicitarios o de elaboración de perfiles de niñas, niños y adolescentes.

La implementación de mecanismos de seguridad no podrá implicar vigilancia generalizada o indiscriminada de la actividad digital de niñas, niños y adolescentes.

CAPÍTULO III: CERTIFICACIÓN Y AUDITORÍA

Artículo 8° — Auditoría y Evaluación

La obtención y renovación del “Sello Espacio Seguro Digital” requerirá una evaluación técnica destinada a verificar el cumplimiento efectivo de los estándares establecidos por la presente ley y su reglamentación.

La evaluación podrá comprender:

- a) La revisión de la infraestructura y configuración de las redes institucionales;
- b) La verificación del funcionamiento de los mecanismos de filtrado y control de contenidos;
- c) La evaluación de las medidas de seguridad implementadas en redes y dispositivos;
- d) La revisión de las políticas y procedimientos de protección de datos y privacidad;
- e) La verificación de los protocolos de gestión de incidentes;
- f) La acreditación de la capacitación del personal correspondiente.

La evaluación deberá verificar, mediante procedimientos técnicos adecuados, que las medidas de seguridad implementadas funcionen efectivamente y no se limiten a su mera existencia documental.

La auditoría deberá realizarse respetando la privacidad de las personas usuarias y sin acceder innecesariamente a contenidos, comunicaciones o datos personales.

Artículo 9º — Certificadores

La autoridad de aplicación establecerá un registro de organismos, entidades o profesionales habilitados para realizar las auditorías.

Los certificadores deberán acreditar idoneidad técnica, independencia y ausencia de conflictos de intereses.

Artículo 10 — Vigencia

La certificación tendrá una vigencia máxima de dos (2) años y deberá renovarse mediante una nueva evaluación.

La autoridad de aplicación podrá establecer controles intermedios de acuerdo con el nivel de certificación y riesgo de la institución.

Artículo 11 — Suspensión y revocación

El Sello podrá ser suspendido o revocado ante incumplimientos graves de los estándares, falsedad de la información presentada, adulteración de informes de auditoría o utilización indebida de la certificación.

La reglamentación establecerá el procedimiento correspondiente, garantizando el derecho de defensa.

CAPÍTULO IV: REGISTRO E INCENTIVOS

Artículo 12 — Registro Nacional

Créase el Registro Nacional de Espacios Seguros Digitales, que tendrá carácter público y contendrá la identificación de las instituciones certificadas, nivel de certificación, fecha de otorgamiento y fecha de vencimiento.

El Registro no podrá contener datos personales de niñas, niños y adolescentes ni información técnica que pueda comprometer la seguridad de las instituciones.

Artículo 13 — Niveles de certificación

La autoridad de aplicación podrá establecer distintos niveles de certificación de acuerdo con el grado de cumplimiento de los estándares, el nivel de madurez de la infraestructura de seguridad digital, las características de la institución y el nivel de protección alcanzado.

Los niveles de certificación deberán contemplar requisitos progresivos y proporcionales, de manera que puedan ser alcanzados por instituciones de diferentes dimensiones y capacidades técnicas.

La reglamentación establecerá los requisitos correspondientes a cada nivel.

Artículo 14 — Incentivos

El Estado Nacional promoverá programas destinados a facilitar la incorporación y permanencia de las instituciones en el Sistema Nacional de Certificación “Espacio Seguro Digital”.

A tal efecto, podrán establecerse:

- a) Programas de asistencia técnica;
- b) Capacitaciones gratuitas;
- c) Provisión o financiamiento de herramientas tecnológicas;
- d) Líneas de financiamiento o subsidios destinados a la adecuación de infraestructura;
- e) Convenios de cooperación con universidades, organismos públicos y entidades especializadas.

Las medidas de asistencia y financiamiento deberán priorizar a las instituciones educativas, deportivas, recreativas y comunitarias que cuenten con menores recursos técnicos o económicos.

CAPÍTULO V: AUTORIDAD DE APLICACIÓN

Artículo 15 — Autoridad de aplicación

El Poder Ejecutivo Nacional determinará la autoridad de aplicación, que deberá coordinar sus acciones con los organismos competentes en materia de educación, niñez y adolescencia, deportes, protección de datos personales y ciberseguridad.

Artículo 16 — Complementariedad normativa

La presente ley complementa las normas vigentes en materia de protección integral de niñas, niños y adolescentes, prevención y abordaje de las violencias digitales, protección de datos personales, educación, deportes y ciberseguridad.

La implementación del Sistema Nacional de Certificación "Espacio Seguro Digital" no sustituye, modifica ni limita las obligaciones, competencias, protocolos o mecanismos de prevención, detección, denuncia y abordaje establecidos por la legislación vigente.

El Sistema tendrá por objeto específico evaluar y certificar las condiciones técnicas y organizativas de seguridad digital de las instituciones, sin constituir un régimen autónomo de prevención o sanción de las conductas comprendidas en otras normas.

Artículo 17 — Coordinación federal

La autoridad de aplicación promoverá mecanismos de cooperación con las provincias y la Ciudad Autónoma de Buenos Aires para favorecer la adopción de estándares comunes y la implementación del Sistema.

CAPÍTULO VI: DISPOSICIONES FINALES

Artículo 18 — Reglamentación

El Poder Ejecutivo Nacional reglamentará la presente ley dentro de los ciento ochenta (180) días de su publicación.

La reglamentación establecerá los estándares técnicos, categorías de contenidos, requisitos de auditoría, niveles de certificación, contenidos mínimos de capacitación y demás aspectos necesarios para su implementación.

Artículo 19 — Comuníquese al Poder Ejecutivo Nacional.

CRISTIAN FELIPE ANDINO

LAURA MARCLAY

RAUL HADAD

PAULO TITA

EDUARDO VALDES

FUNDAMENTOS

Señor Presidente:

El acceso a Internet se ha convertido en una herramienta indispensable para la educación, el deporte, la comunicación y la socialización de niñas, niños y adolescentes. Las instituciones educativas, deportivas, recreativas y formativas son, cada vez con mayor frecuencia, espacios de acceso cotidiano a redes inalámbricas, dispositivos y servicios digitales.

Esta realidad genera una responsabilidad adicional: no alcanza con promover un uso responsable de la tecnología si los propios espacios institucionales en los que niñas, niños y adolescentes se conectan no cuentan con condiciones mínimas y verificables de seguridad.

Los riesgos digitales ya forman parte de situaciones concretas ocurridas en nuestro país. Se han registrado casos de grooming vinculados con docentes y adultos que desarrollaban actividades en instituciones frecuentadas por menores, circulación de imágenes íntimas y contenidos sexuales generados mediante herramientas digitales, acceso de menores a contenidos pornográficos y una creciente participación de adolescentes en plataformas de apuestas online.

Estos hechos demuestran que la protección de niñas, niños y adolescentes requiere una mirada integral que contemple no solamente las conductas individuales, sino también las condiciones de seguridad de los entornos digitales en los que esas conductas pueden producirse.

En este sentido, resulta necesario distinguir entre dos dimensiones complementarias.

Por un lado, existen políticas destinadas a prevenir, detectar y abordar situaciones de bullying, cyberbullying y violencia digital, mediante protocolos, capacitación, mecanismos de intervención y articulación institucional.

Por otro lado, existe una dimensión hasta ahora insuficientemente abordada: la seguridad técnica de la infraestructura digital de las instituciones que proporcionan conectividad a niñas, niños y adolescentes.

La reciente presentación que realice del proyecto de ley denominado "Ley Florencia" —Expediente 3564-D-2026—, constituye un antecedente relevante en materia de prevención, detección temprana y abordaje integral del bullying, ciberbullying y las violencias digitales contra niñas, niños y adolescentes. El proyecto fue girado a las comisiones de Educación, Familias, Niñez y Juventudes, Comunicaciones e Informática y Presupuesto y Hacienda.

La presente iniciativa no pretende sustituir, modificar ni duplicar ese régimen ni ninguna otra normativa vigente. Su finalidad es complementaria y específica: establecer un sistema nacional que permita evaluar y certificar las condiciones técnicas y organizativas de seguridad digital de las instituciones.

El Sello "Espacio Seguro Digital" propone reconocer a aquellas instituciones que acrediten, mediante una evaluación independiente, el cumplimiento de estándares objetivos relativos a la seguridad de sus redes, filtrado de contenidos, protección de dispositivos, privacidad, gestión de accesos, capacitación del personal y respuesta ante incidentes de seguridad.

La propuesta parte de una premisa sencilla: si una institución ofrece conectividad a niñas, niños y adolescentes, debe poder demostrar que ha adoptado medidas razonables para que esa conectividad se encuentre protegida.

Entre los estándares mínimos se contempla la implementación de mecanismos de filtrado y control de contenidos destinados a restringir el acceso, desde las redes institucionales, a categorías incompatibles con la edad de sus usuarios, incluyendo contenidos pornográficos, material de abuso sexual infantil, sitios de apuestas y otras categorías que determine la reglamentación.

También se prevén medidas destinadas a reducir riesgos vinculados con malware, phishing, sitios maliciosos y otras amenazas informáticas, así como mecanismos adecuados de protección de datos personales.

La iniciativa reconoce, al mismo tiempo, que seguridad no significa vigilancia.

Por ello, establece límites expresos respecto del tratamiento de los registros técnicos de conexión y prohíbe su utilización con fines comerciales, publicitarios o de elaboración de perfiles de niñas, niños y adolescentes. Las medidas de seguridad deberán respetar los principios de finalidad, proporcionalidad, minimización y privacidad establecidos por la legislación vigente.

Otro componente central es la auditoría independiente.

El Sello no deberá otorgarse simplemente por la presentación de una declaración institucional. Será necesario acreditar, mediante procedimientos técnicos adecuados, que las medidas implementadas funcionan efectivamente.

La certificación tendrá una vigencia limitada y deberá renovarse periódicamente, permitiendo así que el sistema acompañe la evolución de las tecnologías y de las amenazas digitales.

Asimismo, se establece un criterio de proporcionalidad. No resulta razonable exigir idénticos recursos tecnológicos a una gran institución educativa que a un pequeño club deportivo o una organización comunitaria. Por ello, los estándares deberán adecuarse al tamaño, infraestructura, cantidad de usuarios y nivel de riesgo de cada institución.

El proyecto incorpora además a los clubes y entidades deportivas, reconociendo que la protección digital no puede circunscribirse exclusivamente al ámbito escolar. Niñas, niños y adolescentes desarrollan buena parte de sus actividades cotidianas en clubes,

asociaciones y espacios recreativos y formativos que también utilizan dispositivos y conectividad.

El carácter voluntario del Sistema busca que el “Sello Espacio Seguro Digital” funcione inicialmente como un estándar de calidad y confianza, generando incentivos para que las instituciones mejoren progresivamente sus condiciones de seguridad.

El Estado Nacional podrá acompañar este proceso mediante asistencia técnica, capacitación, financiamiento y provisión de herramientas, priorizando a las instituciones que cuenten con menores recursos.

La propuesta se basa, en consecuencia, en cuatro pilares que son seguridad de la infraestructura, protección de la privacidad, capacitación y auditoría independiente.

No se pretende crear un nuevo régimen general de regulación de Internet ni trasladar a las instituciones responsabilidades que corresponden a las plataformas digitales, a los proveedores de conectividad o a las autoridades competentes.

Se busca algo concreto y verificable: que una institución que trabaja con niñas, niños y adolescentes pueda demostrar que sus redes y sistemas cumplen condiciones adecuadas de seguridad digital.

De esta manera, el “Sello Espacio Seguro Digital” puede constituir una herramienta complementaria a las políticas de prevención y abordaje de las violencias digitales, fortaleciendo un aspecto diferente pero indispensable de la protección integral: la seguridad del entorno tecnológico institucional.

Por todo lo expuesto, solicitamos a nuestros pares la aprobación del presente proyecto de ley.

CRISTIAN FELIPE ANDINO
LAURA MARCLAY

RAUL HADAD
PAULO TITA
EDUARDO VALDES