PROYECTO DE LEY

EL SENADO Y LA CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA SANCIONAN CON FUERZA DE

LEY

LEY DE CIBERSEGURIDAD NACIONAL Y CREACIÓN DEL CENTRO NACIONAL DE CIBERSEGURIDAD

TÍTULO I — DISPOSICIONES GENERALES

ARTÍCULO 1° — Objeto. La presente ley crea el Centro Nacional de Ciberseguridad (CNCiber) como autoridad nacional rectora en materia de ciberseguridad, con las misiones y funciones establecidas en la presente norma, dotado de competencias de coordinación, regulación técnica y articulación interinstitucional a nivel federal.

Asimismo, la presente ley establece las obligaciones de los sujetos alcanzados por su ámbito de aplicación, el régimen de respuesta a incidentes, la protección de infraestructuras críticas, las garantías de privacidad y derechos digitales, y el régimen sancionatorio aplicable al incumplimiento de sus disposiciones.

El ejercicio de dichas competencias se realizará sin alterar la distribución de funciones establecida por las Leyes N° 24.059 de Seguridad Interior, 23.554 de Defensa Nacional y 25.520 de Inteligencia Nacional, en el marco de un sistema integrado de ciberseguridad nacional.

ARTÍCULO 2° — Principios Rectores. La presente ley se rige por los siguientes principios:

a) Proporcionalidad: las medidas de seguridad deberán ser adecuadas, necesarias y proporcionales a los riesgos identificados.

b) Gestión de riesgos: la política de ciberseguridad se basará en la evaluación continua, priorización y mitigación de riesgos.

c) Resiliencia: el Estado promoverá la capacidad de anticipar, absorber, adaptarse y recuperarse frente a incidentes cibernéticos.

d) Cooperación: se fomentará la colaboración interinstitucional, público-privada e internacional.

e) Respeto por los derechos fundamentales: toda acción en materia de ciberseguridad deberá respetar los derechos a la privacidad, la intimidad, la libertad de expresión y el debido proceso, conforme la Constitución Nacional, los tratados internacionales de derechos humanos con jerarquía constitucional y la Ley N° 25.326.

f) Transparencia: el Estado informará periódicamente a la ciudadanía sobre el estado de la ciberseguridad nacional, con las reservas que impongan la seguridad nacional y la Ley N° 25.520.

g) Continuidad: se garantizará la continuidad de los servicios esenciales ante la ocurrencia de incidentes cibernéticos.

h) Neutralidad tecnológica: las obligaciones establecidas en esta ley serán tecnológicamente neutrales y no favorecerán soluciones tecnológicas específicas.

i) Responsabilidad compartida: la ciberseguridad es responsabilidad conjunta del Estado, el sector privado, la academia y la ciudadanía, con roles diferenciados según la posición de cada actor en el ecosistema digital.

j) Divulgación responsable: se promoverá un entorno jurídico que incentive la identificación y reporte responsable de vulnerabilidades, proveyendo certeza jurídica a los investigadores de seguridad de buena fe.

ARTÍCULO 3° — Orden Público. Las disposiciones de la presente ley son de orden público y de aplicación en todo el territorio de la República Argentina, sin perjuicio de las competencias que correspondan a las jurisdicciones provinciales y a la Ciudad Autónoma de Buenos Aires, conforme el régimen federal establecido en la Constitución Nacional.

ARTÍCULO 4° — Definiciones. A los efectos de la presente ley, se entiende por:

a) Ciberespacio: entorno digital resultante de la interacción de personas, software, servicios y sistemas a través de redes de comunicaciones electrónicas.

b) Ciberseguridad: conjunto de capacidades humanas, técnicas, organizacionales y jurídicas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información, los sistemas y las redes de comunicaciones electrónicas, así como las infraestructuras que los soportan.

c) Incidente cibernético: todo evento real o potencial que comprometa la seguridad de sistemas informáticos, redes o datos, afectando su confidencialidad, integridad o disponibilidad.

d) Infraestructura Crítica: conjunto de instalaciones, redes, servicios y activos físicos y digitales cuya interrupción o destrucción tendría un impacto grave sobre la seguridad, la salud pública, la economía, el ambiente o el funcionamiento del Estado. Se consideran sectores de infraestructura crítica, de manera enunciativa, los siguientes: energía; transporte y logística; banca, servicios financieros y seguros; salud e industria farmacéutica; agua potable y saneamiento; infraestructura digital y servicios de computación en la nube; servicios de confianza y autenticación; telecomunicaciones; alimentación; espacio; administración pública nacional, provincial y municipal; y seguridad pública y defensa. La reglamentación determinará los operadores específicos dentro de cada sector y podrá incorporar nuevos sectores

mediante resolución fundada del CNCiber, con ratificación del Comité Interministerial.

e) Operador de Infraestructura Crítica (OIC): persona humana o jurídica, pública o privada, que gestiona o administra una infraestructura crítica.

f) Vulnerabilidad: debilidad de un sistema, aplicación o proceso que puede ser explotada por un agente de amenaza.

g) Ciberataque: acción deliberada llevada a cabo en el ciberespacio con el propósito de dañar, destruir, interrumpir, obtener acceso no autorizado o manipular sistemas informáticos, datos o redes.

h) CSIRT (Computer Security Incident Response Team): equipo especializado para la coordinación, análisis y respuesta ante incidentes de seguridad informática.

i) Gestión de riesgos de ciberseguridad: proceso sistemático de identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos asociados al ciberespacio.

j) Divulgación coordinada de vulnerabilidades (CVD): proceso por el cual una persona que ha identificado una vulnerabilidad en un sistema la comunica al responsable del mismo de forma confidencial y dentro de un plazo razonable, con el objeto de que sea corregida antes de su divulgación pública.

k) Cadena de suministro de software: conjunto de proveedores, procesos y componentes de código abierto o propietario que intervienen en el desarrollo, distribución e implementación de software utilizado por sujetos obligados.

l) Lista de Materiales de Software (SBOM): inventario formal y legible por máquina de los componentes, bibliotecas y módulos que conforman un producto de software.

m) Vigilancia masiva: toda recolección, tratamiento o análisis indiscriminado, generalizado o no focalizado de datos, comunicaciones

o actividades en el ciberespacio, sin la existencia de una amenaza concreta, específica y previamente identificada que la justifique.

ARTÍCULO 5° — Articulación Normativa. Las disposiciones de esta ley complementan y no derogan la legislación vigente en materia de datos personales, delitos informáticos, inteligencia nacional, defensa nacional, seguridad interior y acceso a la información pública. En particular, mantienen plena vigencia la Ley N° 25.326, la Ley N° 26.388, la Ley N° 27.411, la Ley N° 27.275, la Ley N° 25.520, la Ley N° 23.554 y la Ley N° 24.059. Ante cualquier conflicto normativo se aplicará el principio de especialidad; en materia de derechos fundamentales, la norma más protectoria para el titular del derecho.

TÍTULO II — SUJETOS OBLIGADOS

ARTÍCULO 6° — Ámbito de Aplicación Subjetivo. Quedan sujetos a las disposiciones de la presente ley:

a) Las entidades de la Administración Pública Nacional comprendidas en el artículo 8° de la Ley N° 24.156.

b) Los Poderes Legislativo y Judicial de la Nación y el Ministerio Público, en lo que respecta a sus sistemas informáticos y redes de comunicación, sin afectar su independencia constitucional. La determinación de las medidas técnicas aplicables a dichos poderes se realizará mediante acuerdo interinstitucional, con intervención del CNCiber en carácter consultivo.

c) Los operadores de infraestructuras críticas, en los términos del artículo 4°, inciso (e) de la presente ley.

d) Los proveedores de servicios digitales esenciales —incluyendo servicios de computación en la nube, motores de búsqueda, plataformas de comercio electrónico y redes de distribución de contenidos— que superen los umbrales de tamaño o criticidad que establezca la reglamentación y operen en el territorio nacional.

e) Las organizaciones privadas de los sectores enumerados en el artículo 4°, inciso (d), que sean declarados OIC conforme el procedimiento reglamentario.

f) Los proveedores críticos de tecnología de la información y comunicaciones del Estado Nacional, conforme el registro que establezca el CNCiber.

Las jurisdicciones provinciales y la Ciudad Autónoma de Buenos Aires serán invitadas a adherir a los estándares mínimos de ciberseguridad establecidos en el marco de la presente ley.

ARTÍCULO 7° — Obligaciones Generales de los Sujetos Obligados. Los sujetos indicados en el artículo 6° deberán:

a) Implementar un sistema de gestión de riesgos de ciberseguridad adecuado a su tamaño, complejidad y criticidad, basado en los marcos de referencia reconocidos por el CNCiber.

b) Designar un responsable de ciberseguridad (CISO) o equivalente, con las competencias y nivel jerárquico que determine la reglamentación según el tamaño y criticidad del sujeto obligado.

c) Elaborar y mantener actualizado un plan de continuidad operativa y recuperación ante incidentes cibernéticos.

d) Notificar al CNCiber todo incidente cibernético significativo dentro de las veinticuatro (24) horas de su detección, con informe técnico complementario dentro de las setenta y dos (72) horas, conforme el procedimiento reglamentario.

e) Cooperar con el CNCiber y las autoridades competentes en la investigación y gestión de incidentes.

f) Adoptar, como mínimo, las siguientes medidas técnicas de seguridad: (i) autenticación multifactor para acceso a sistemas críticos; (ii) cifrado de datos en tránsito y en reposo para información clasificada o sensible; (iii) segmentación de redes críticas; (iv) gestión de parches y actualizaciones de seguridad en plazos definidos por el CNCiber; (v) realización de copias de seguridad periódicas con verificación de

integridad; (vi) gestión de identidades y accesos con principio de mínimo privilegio; y (vii) registro y monitoreo de eventos de seguridad (logs). El CNCiber podrá establecer medidas adicionales mediante resolución fundada, respetando el principio de proporcionalidad.

g) Realizar evaluaciones de vulnerabilidad y pruebas de penetración con la periodicidad que establezca la reglamentación, mediante personal habilitado o terceros certificados.

h) Capacitar periódicamente a su personal en materia de ciberseguridad y concientización digital.

i) Conservar los registros de eventos de seguridad (logs) por el período que establezca la reglamentación, con un mínimo de doce (12) meses, garantizando su integridad, autenticidad y trazabilidad, y respetando la Ley N° 25.326.

j) Contar con una política interna de divulgación de vulnerabilidades (VDP) que establezca los canales y procedimientos para el reporte de vulnerabilidades por terceros, en concordancia con el artículo 21 bis° de la presente ley.

TÍTULO III — CENTRO NACIONAL DE CIBERSEGURIDAD

ARTÍCULO 8° — Creación. Créase el Centro Nacional de Ciberseguridad (CNCiber) como organismo descentralizado en el ámbito de la Jefatura de Gabinete de Ministros de la Nación, con autarquía funcional, personería jurídica propia y plena capacidad de actuación en el ámbito del derecho público y privado. El CNCiber gozará de independencia técnica y operativa en el ejercicio de sus funciones.

ARTÍCULO 9° — Misión y Funciones. El CNCiber tendrá las siguientes misiones y funciones:

a) Diseñar, coordinar, implementar y evaluar la Estrategia Nacional de Ciberseguridad.

b) Actuar como autoridad nacional de referencia y punto de contacto en materia de ciberseguridad ante organismos internacionales y otros Estados.

c) Operar el CSIRT Nacional, coordinando la respuesta ante incidentes cibernéticos que afecten a los sujetos obligados o a la seguridad nacional, con estricto respeto del derecho a la privacidad de las comunicaciones. El monitoreo de tráfico de redes privadas solo procederá con autorización judicial previa o con consentimiento expreso, específico e informado del titular del sistema, el cual será revocable en cualquier momento.

d) Supervisar el cumplimiento de las obligaciones establecidas en la presente ley por parte de los sujetos obligados.

e) Establecer estándares y medidas técnicas adicionales de seguridad de obligatorio cumplimiento, dentro del marco de las medidas mínimas establecidas por el artículo 7°, inciso f), de la presente ley.

f) Elaborar y publicar guías, marcos de referencia y mejores prácticas en la materia.

g) Promover la investigación, el desarrollo tecnológico y la formación de capacidades en ciberseguridad.

h) Administrar el Registro Nacional de Incidentes Cibernéticos.

i) Coordinar con las Fuerzas de Seguridad y el Poder Judicial para la investigación de ciberdelitos, en el marco de la Ley N° 26.388 y la Ley N° 27.411.

j) Emitir alertas tempranas y recomendaciones ante amenazas identificadas.

k) Fomentar la cooperación internacional en materia de ciberseguridad, con sujeción a la política exterior de la Nación.

l) Promover la adhesión de las provincias y la Ciudad Autónoma de Buenos Aires a los estándares nacionales.

m) Administrar el sistema nacional de divulgación coordinada de vulnerabilidades (CVD), conforme el artículo 21 bis° de la presente ley.

n) Gestionar y publicar el Registro Nacional de Proveedores Críticos TIC del Estado, conforme el artículo 21 ter° de la presente ley.

o) El CNCiber no ejercerá funciones de investigación criminal, inteligencia interior ni tareas propias de las fuerzas de seguridad. Podrá brindar asistencia técnica especializada en el marco de investigaciones judiciales, a requerimiento de autoridad judicial competente, sin asumir funciones de policía judicial ni subordinarse operativamente a las fuerzas de seguridad.

ARTÍCULO 10° — Integración. El CNCiber estará conducido por un Director Nacional designado por el Poder Ejecutivo Nacional a propuesta del Jefe de Gabinete de Ministros, con rango de Secretario. Para acceder al cargo, el candidato deberá acreditar formación superior y experiencia mínima de cinco (5) años en ciberseguridad o disciplinas afines, y no podrá registrar antecedentes penales por delitos dolosos ni haber ejercido actividad de representación comercial de empresas de tecnología durante los dos (2) años inmediatos anteriores a su designación.

Se conformará un Comité Interministerial de Ciberseguridad integrado por representantes de los siguientes organismos:

a) Ministerio de Seguridad de la Nación;

b) Ministerio de Defensa;

c) Ministerio del Interior;

d) Ministerio de Economía;

e) Ministerio de Relaciones Exteriores, Comercio Internacional y Culto;

f) Agencia Federal de Inteligencia (AFI), exclusivamente a los fines de intercambio de información estratégica en el marco de la Ley N° 25.520, sin facultades operativas en el ámbito del CNCiber;

g) Unidad de Información Financiera (UIF);

h) Secretaría de Asuntos Estratégicos de la Presidencia de la Nación;

i) Ente Nacional de Comunicaciones (ENACOM);

j) Agencia de Acceso a la Información Pública.

El Comité funcionará como órgano consultivo y de coordinación estratégica, sin perjuicio de las competencias específicas de cada organismo.

ARTÍCULO 11° — Consejo Consultivo. Créase un Consejo Consultivo ad honorem conformado por representantes del sector académico, de la industria tecnológica nacional, de organizaciones de la sociedad civil con expertise en seguridad digital y derechos digitales, de Colegios Profesionales vinculados a las tecnologías de la información, y de investigadores de seguridad independientes. Sus funciones serán de asesoramiento no vinculante. La integración y funcionamiento se determinarán reglamentariamente, garantizando la pluralidad de perspectivas, la ausencia de conflictos de interés y cobertura de gastos de funcionamiento.

El Consejo Consultivo deberá ser consultado obligatoriamente antes de la aprobación de: (i) la Estrategia Nacional de Ciberseguridad; (ii) las medidas técnicas de cumplimiento obligatorio que excedan las previstas en el artículo 7° inc. f); y (iii) el régimen de divulgación coordinada de vulnerabilidades.

ARTÍCULO 12° — Transparencia y Rendición de Cuentas. El CNCiber publicará anualmente un informe de gestión y estado de la ciberseguridad nacional, con los alcances y reservas que establezca la Ley N° 25.520 y la reglamentación de la presente ley. El informe estará disponible en el portal oficial y será remitido al Honorable Congreso de la Nación dentro de los noventa (90) días de cerrado el ejercicio anual.

El informe anual deberá incluir, como mínimo:

a) estadísticas de incidentes notificados por sector y severidad, de forma anonimizada;

b) estado de cumplimiento de los sujetos obligados;

c) resultados de auditorías realizadas, de forma agregada;

d) actividades de la red de CSIRTs;

e) estado de la cooperación internacional;

f) avance en los objetivos de la Estrategia Nacional de Ciberseguridad; y

g) evaluación de la actividad de la Comisión Bicameral de Supervisión.

TÍTULO III bis — CONTROL PARLAMENTARIO

ARTÍCULO 12 bis° — Comisión Bicameral de Supervisión de la Ciberseguridad Nacional. Créase la Comisión Bicameral de Supervisión de la Ciberseguridad Nacional (CBSCN), integrada por seis (6) senadores nacionales y seis (6) diputados nacionales, designados por los presidentes de las respectivas .Cámaras en proporción a la representación de los bloques parlamentarios.

La Comisión Bicameral tendrá las siguientes funciones:

a) Supervisar el funcionamiento del CNCiber y el cumplimiento de los objetivos de la Estrategia Nacional de Ciberseguridad.

b) Recibir y analizar el informe anual del CNCiber y emitir dictamen dentro de los sesenta (60) días.

c) Convocar al Director Nacional del CNCiber y a los miembros del Comité Interministerial para informar sobre materias de su competencia.

d) Tomar conocimiento de las actividades de monitoreo de redes del CNCiber y verificar su conformidad con las disposiciones de la presente ley y la Ley N° 25.326.

e) Recibir informes clasificados sobre incidentes de ciberseguridad de alta criticidad, bajo las reservas de confidencialidad que correspondan conforme la Ley N° 25.520.

f) Dictaminar sobre proyectos de actos administrativos del CNCiber que impliquen restricción de derechos fundamentales.

g) Proponer al Congreso las adecuaciones legislativas que resulten necesarias ante la evolución tecnológica o la experiencia acumulada en la aplicación de la presente ley.

TÍTULO IV — ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

ARTÍCULO 13° — Estrategia Nacional de Ciberseguridad. El Poder Ejecutivo Nacional, a través del CNCiber y con la participación del Comité Interministerial y el Consejo Consultivo, aprobará mediante decreto una Estrategia Nacional de Ciberseguridad (ENC) que deberá:

a) Establecer objetivos, prioridades y lineamientos estratégicos en materia de ciberseguridad para un horizonte de cuatro (4) años, con revisión bienal.

b) Identificar los sectores críticos y las amenazas prioritarias para la seguridad nacional.

c) Definir roles, responsabilidades y mecanismos de coordinación entre los distintos actores.

d) Establecer metas de desarrollo de capacidades nacionales en ciberseguridad, con indicadores de resultado medibles.

e) Contemplar la dimensión de ciberdefensa, en coordinación con el Ministerio de Defensa y la Ley N° 23.554.

f) Incorporar los compromisos derivados del Convenio de Budapest y demás instrumentos internacionales ratificados por la Argentina.

g) Promover el desarrollo de la industria nacional de ciberseguridad y la soberanía tecnológica.

h) Incluir una política nacional de seguridad de la cadena de suministro de software y hardware para el Estado Nacional.

ARTÍCULO 14° — Ciberdefensa. Sin perjuicio de las misiones y funciones del CNCiber, la ciberdefensa —entendida como la protección del ciberespacio ante agresiones de actores estatales extranjeros y como la capacidad de respuesta del Estado en ese ámbito— quedará bajo la competencia del Ministerio de Defensa y las Fuerzas Armadas, en los términos de la Ley N° 23.554, coordinando con el CNCiber los aspectos que requieran respuesta interagencial. El CNCiber y el Ministerio de Defensa suscribirán un protocolo de coordinación operativa dentro de los noventa (90) días de entrada en vigor de la presente ley.

Las actividades de ciberdefensa ofensiva —si las hubiere— quedarán sujetas a las limitaciones y controles establecidos en la Ley N° 23.554, la Ley N° 25.520, el derecho internacional humanitario aplicable y la Carta de las Naciones Unidas.

TÍTULO V — PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

ARTÍCULO 15° — Registro de Operadores de Infraestructuras Críticas. El CNCiber mantendrá un Registro Nacional de Operadores de Infraestructuras Críticas (RNOIC). La inclusión en el registro será obligatoria para los operadores identificados conforme el artículo 4°, inciso (e). El registro será confidencial en su contenido, aunque su existencia y los sectores representados en él serán públicos. El procedimiento de inclusión, exclusión e impugnación de la clasificación se establecerá reglamentariamente, garantizando el derecho de defensa y el control judicial posterior.

ARTÍCULO 16° — Obligaciones Específicas de los Operadores de Infraestructuras Críticas. Además de las obligaciones del artículo 7°, los OIC deberán:

a) Realizar una evaluación de riesgos de ciberseguridad anual y remitir un resumen al CNCiber.

b) Implementar las medidas de seguridad específicas que establezca el CNCiber para su sector, con base en los marcos de referencia internacionales aplicables.

c) Realizar ejercicios de respuesta a incidentes con una periodicidad no superior a dos (2) años, con participación del CNCiber cuando este lo requiera.

d) Notificar incidentes significativos dentro de las veinticuatro (24) horas, con informe complementario dentro de las setenta y dos (72) horas y un informe final dentro de un mes.

e) Garantizar la seguridad de su cadena de suministro digital, adoptando medidas de verificación de proveedores de tecnología que incluyan la exigencia de SBOM para los proveedores de software crítico.

f) Designar un punto de contacto permanente ante el CNCiber disponible en todo momento para la gestión de incidentes.

g) Asegurar que los sistemas de control industrial (SCADA/ICS) que operen infraestructuras críticas físicas se encuentren segmentados de redes de acceso general y cumplan los estándares IEC 62443 o equivalentes reconocidos por el CNCiber.

ARTÍCULO 17° — Auditorías. El CNCiber podrá realizar o encargar auditorías de ciberseguridad a los sujetos obligados, con ajuste a los principios de proporcionalidad, no intromisión indebida y respeto a los secretos comerciales e industriales. Las auditorías deberán ser realizadas por personal habilitado o por terceros certificados por el CNCiber. Los resultados serán reservados salvo las comunicaciones que la reglamentación autorice.

Los sujetos obligados que acrediten haber completado voluntariamente una auditoría certificada por el CNCiber dentro del año previo quedarán eximidos de la auditoría obligatoria de ese período, salvo que el CNCiber

justifique su realización por razones específicas de seguridad nacional o ante incidentes ocurridos.

Las auditorías que impliquen acceso a sistemas o información sensible de sujetos privados requerirán orden judicial previa, salvo consentimiento expreso del titular del sistema.

TÍTULO VI — RESPUESTA A INCIDENTES

ARTÍCULO 18° — CSIRT Nacional. El CNCiber operará el CSIRT Nacional como unidad especializada en la prevención, detección, análisis y respuesta coordinada ante incidentes de ciberseguridad a escala nacional. El CSIRT Nacional actuará como punto de contacto ante la Red de CSIRTs gubernamentales nacionales e internacionales, incluyendo el CERT.br de Brasil, el CSIRT de Chile y la red FIRST (Forum of Incident Response and Security Teams).

El CSIRT Nacional desarrollará sus actividades con pleno respeto del derecho a la privacidad de las comunicaciones. El tratamiento de datos personales en el marco de la gestión de incidentes se regirá por el principio de minimización y se ajustará a lo establecido en la Ley N° 25.326.

ARTÍCULO 19° — Red Nacional de CSIRTs. El CNCiber promoverá la creación de una red de CSIRTs sectoriales —en los sectores de salud, finanzas, energía, transporte y defensa, entre otros— que actuarán de forma coordinada con el CSIRT Nacional. Las provincias y la Ciudad Autónoma de Buenos Aires podrán integrar la red mediante convenios de adhesión. El CNCiber brindará asistencia técnica y financiera para el desarrollo de los CSIRTs provinciales que así lo requieran.

ARTÍCULO 20° — Notificación de Incidentes. Todo sujeto obligado deberá notificar al CSIRT Nacional los incidentes cibernéticos que afecten la disponibilidad, integridad o confidencialidad de sus sistemas o datos dentro del plazo de veinticuatro (24) horas de su detección. La

reglamentación establecerá los criterios de significatividad, el procedimiento de notificación y los umbrales de afectación.

La información contenida en las notificaciones de incidentes tendrá carácter reservado y solo podrá ser utilizada para los fines de gestión y prevención de incidentes. No podrá ser utilizada como prueba en procedimientos sancionatorios contra el sujeto notificante, salvo que el incidente haya sido causado por dolo o negligencia grave de ese sujeto.

La obligación de notificación al CNCiber es independiente y compatible con la obligación de notificación a la Agencia de Acceso a la Información Pública ante vulneraciones de datos personales, conforme la Ley N° 25.326. En caso de vulneración que afecte simultáneamente la seguridad del sistema y datos personales, se admitirá notificación única con efectos para ambas obligaciones.

ARTÍCULO 21° — Coordinación con las Fuerzas de Seguridad. Cuando un incidente cibernético revista carácter delictivo, el CNCiber articulará con las Fuerzas de Seguridad y el Ministerio Público Fiscal, preservando la cadena de custodia de la evidencia digital conforme a los estándares del Convenio de Budapest, su Segundo Protocolo Adicional, y la Ley N° 26.388. El CNCiber colaborará con la unidad fiscal especializada en cibercrimen de la Procuración General de la Nación, sin subordinación a ella y sin perjuicio de la independencia del Ministerio Público.

La evidencia digital obtenida por el CNCiber en el ejercicio de sus funciones de prevención y respuesta a incidentes solo podrá ser utilizada en procedimientos penales con autorización judicial, preservando las garantías del artículo 18° de la Constitución Nacional.

ARTÍCULO 21 bis° — Divulgación Coordinada de Vulnerabilidades. El Centro Nacional de Ciberseguridad (CNCiber) administrará un sistema nacional de divulgación coordinada de vulnerabilidades (Coordinated Vulnerability Disclosure – CVD), destinado a facilitar la identificación, comunicación y corrección de vulnerabilidades en los sistemas informáticos de los sujetos obligados.

La investigación de seguridad informática realizada de buena fe con la finalidad exclusiva de identificar, analizar o reportar vulnerabilidades en sistemas informáticos de sujetos obligados no será considerada acceso ilegítimo ni conducta penalmente reprochable, siempre que se cumplan conjuntamente las siguientes condiciones:

a) Que la actividad se realice con el único propósito de detectar, verificar o reportar una vulnerabilidad de seguridad.

b) Que el investigador actúe de buena fe y sin intención de causar daño, obtener un beneficio indebido o explotar la vulnerabilidad identificada.

c) Que el acceso o interacción con el sistema se limite estrictamente a lo necesario para comprobar la existencia de la vulnerabilidad.

d) Que la vulnerabilidad sea reportada de forma inmediata, confidencial y completa al responsable del sistema afectado o al CNCiber, conforme los procedimientos establecidos por la reglamentación.

e) Que el investigador se abstenga de alterar, destruir o divulgar datos contenidos en el sistema, salvo en la medida estrictamente necesaria para demostrar la existencia de la vulnerabilidad.

f) Que no se proceda a la divulgación pública de la vulnerabilidad antes de transcurrido un plazo razonable para su corrección, el cual no podrá ser inferior a noventa (90) días desde la notificación, salvo acuerdo con el responsable del sistema o resolución fundada del CNCiber.

El cumplimiento de las condiciones precedentes constituirá una circunstancia eximente de responsabilidad penal y civil respecto de las conductas estrictamente necesarias para la identificación y reporte de la vulnerabilidad, sin perjuicio de las responsabilidades que pudieran corresponder por actos que excedan dichos límites.

La reglamentación establecerá el procedimiento del sistema de divulgación coordinada de vulnerabilidades, los canales oficiales de reporte, los plazos

de respuesta de los sujetos obligados y las condiciones técnicas aplicables a los investigadores de seguridad.

ARTÍCULO 21 ter° — Seguridad de la Cadena de Suministro del Estado. El CNCiber mantendrá un Registro Nacional de Proveedores Críticos TIC del Estado (RNPTIC), en el que deberán inscribirse los proveedores de software, hardware y servicios de nube que presten servicios a los sujetos obligados del artículo 6°, incisos a) y b), y que superen los umbrales de criticidad que establezca la reglamentación.

Los proveedores incluidos en el RNPTIC deberán: a) entregar una Lista de Materiales de Software (SBOM) en formatos estandarizados reconocidos internacionalmente; b) notificar al CNCiber dentro de las cuarenta y ocho (48) horas cualquier vulnerabilidad conocida en los productos que provean al Estado; c) mantener un plan de gestión de vulnerabilidades y parches con plazos de remediación definidos; d) permitir auditorías de seguridad de código fuente o equivalentes cuando el CNCiber las requiera fundadamente; y e) no subcontratar funciones críticas sin previa comunicación al CNCiber.

La contratación de proveedores TIC por parte del Estado Nacional quedará condicionada al cumplimiento de las obligaciones establecidas en el presente artículo, siendo condición de elegibilidad en los procedimientos de contratación pública.

TÍTULO VII — PRIVACIDAD Y DERECHOS DIGITALES

ARTÍCULO 22° — Protección de Datos Personales. Las actividades desarrolladas en el marco de la presente ley deberán ajustarse en todo momento a la Ley N° 25.326 de Protección de los Datos Personales, su decreto reglamentario y las disposiciones de la Agencia de Acceso a la Información Pública. La recopilación, tratamiento y conservación de datos personales en el ejercicio de funciones de ciberseguridad deberá observar

los principios de minimización, finalidad, proporcionalidad y limitación temporal.

Los datos personales obtenidos en la gestión de incidentes no podrán ser conservados por el CNCiber por un plazo superior al estrictamente necesario para los fines de prevención y respuesta, con un máximo de cinco (5) años, salvo que su conservación sea ordenada por autoridad judicial competente.

ARTÍCULO 23° — Derechos Fundamentales en el Ciberespacio. Ninguna medida adoptada en virtud de la presente ley podrá vulnerar el derecho a la intimidad, a la privacidad de las comunicaciones, a la libertad de expresión ni al debido proceso, reconocidos en la Constitución Nacional y en los instrumentos internacionales de derechos humanos con jerarquía constitucional. Toda restricción de derechos fundamentales deberá contar con autorización judicial previa, salvo situaciones de urgencia debidamente fundadas y sujetas a control judicial ulterior inmediato, el que deberá producirse dentro de las cuarenta y ocho (48) horas de adoptada la medida de urgencia.

ARTÍCULO 24° — Prohibición de Vigilancia Masiva. Queda expresamente prohibido el uso de las facultades y recursos del CNCiber para la vigilancia masiva, sistemática e indiscriminada de comunicaciones o actividades de personas en el ciberespacio, tanto en redes públicas como privadas. Las tareas de monitoreo activo se limitarán estrictamente a: a) las redes e infraestructuras de los sujetos obligados del artículo 6° incisos a) y b), previo acuerdo formal; b) los sistemas respecto de los cuales exista una amenaza específica, identificable y documentada; o c) los sistemas respecto de los cuales exista orden judicial fundada.

Toda actividad de monitoreo deberá ser registrada con identificación del sistema monitoreado, la base legal habilitante, el período y el personal autorizado. Dichos registros serán auditables por la Comisión Bicameral creada por el artículo 12 bis°.

TÍTULO VIII — INVESTIGACIÓN, FORMACIÓN Y COOPERACIÓN

ARTÍCULO 25° — Desarrollo de Capacidades. El Estado Nacional, a través del CNCiber y en coordinación con los ministerios competentes, promoverá: a) La incorporación de la educación en ciberseguridad en todos los niveles del sistema educativo; b) La formación de profesionales especializados mediante programas universitarios y de posgrado; c) El desarrollo de certificaciones nacionales de ciberseguridad, reconocidas internacionalmente; d) La investigación científica y tecnológica aplicada en la materia, en articulación con el CONICET, las universidades nacionales y el sector privado; e) La generación de incentivos fiscales y de compra pública preferencial para el desarrollo de la industria nacional de ciberseguridad; f) Programas específicos de formación para el Poder Judicial y el Ministerio Público en materia de evidencia digital y ciberdelincuencia.

ARTÍCULO 26° — Cooperación Internacional. El CNCiber, en coordinación con el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, promoverá y gestionará la cooperación bilateral y multilateral en materia de ciberseguridad, incluyendo el intercambio de información sobre amenazas, la asistencia técnica mutua, la participación en ejercicios internacionales y la armonización normativa en el marco del Convenio de Budapest, su Segundo Protocolo Adicional, la UIT, la OEA y demás foros internacionales pertinentes. Se priorizará la cooperación en el marco del MERCOSUR, la CELAC y el esquema de respuesta a incidentes de la OEA/CITEL.

ARTÍCULO 27° — Cooperación Público-Privada. El CNCiber establecerá mecanismos formales de cooperación con el sector privado para el intercambio de información sobre amenazas e incidentes, fomentando la creación de centros de análisis e intercambio de información (ISAC)

sectoriales. La participación del sector privado en dichos mecanismos será voluntaria. La información compartida por el sector privado en el marco de estos mecanismos gozará de las reservas de confidencialidad que establezca la reglamentación y no podrá ser utilizada como prueba en procedimientos administrativos sancionatorios contra la entidad que la aportó, salvo que exista obligación legal de notificación incumplida.

TÍTULO IX — RÉGIMEN SANCIONATORIO

ARTÍCULO 28° — Infracciones Administrativas. El incumplimiento de las obligaciones establecidas en los artículos 7° y 16° de la presente ley por parte de los sujetos obligados, sin perjuicio de las responsabilidades civiles y penales que pudieren corresponder, dará lugar a las siguientes sanciones administrativas:

a) Apercibimiento, con publicación en el portal oficial del CNCiber.

b) Multa de hasta el equivalente en pesos entre el cero coma cinco por ciento (0,5%) y el cuatro por ciento (4%) de la facturación anual del sujeto obligado del ejercicio anterior. Para los operadores de infraestructuras críticas alcanzados por el artículo 16°, la multa podrá alcanzar hasta el cuatro por ciento (4%) de la facturación. Para los demás sujetos obligados, el máximo será del dos por ciento (2%) de la facturación.

c) Inhabilitación temporal para contratar con el Estado Nacional, de hasta tres (3) años, para sujetos del sector privado en casos de infracciones graves o reiteradas.

d) Para los organismos públicos alcanzados por el artículo 6° incisos a) y b): publicación obligatoria del incumplimiento en el Boletín Oficial y en el portal del CNCiber; comunicación al ministerio o autoridad jerárquica competente para la sustanciación del régimen disciplinario aplicable al responsable de ciberseguridad del organismo; y, en caso de reincidencia, comunicación a la Comisión

Bicameral de Supervisión creada por el artículo 12 bis° de la presente ley.

Las sanciones se graduarán teniendo en cuenta: la gravedad de la infracción y el daño causado o potencial; el tamaño y criticidad del sujeto obligado; la conducta del infractor una vez detectada la infracción; la cooperación con las autoridades; la existencia de antecedentes sancionatorios; y las medidas de remediación adoptadas.

ARTÍCULO 29° — Procedimiento Sancionatorio. Las sanciones administrativas serán aplicadas por el CNCiber, garantizando el derecho de defensa, el debido proceso, el derecho a ofrecer y producir prueba y el control judicial posterior. El procedimiento se regirá por la Ley N° 19.549 de Procedimientos Administrativos y su reglamentación. El plazo de prescripción de las infracciones será de cinco (5) años desde la comisión del hecho o, si este es continuado, desde su cesación.

Las resoluciones sancionatorias del CNCiber serán recurribles ante la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal.

ARTÍCULO 30° — Delitos Informáticos. La comisión de delitos informáticos tipificados en el Código Penal de la Nación conforme la Ley N° 26.388, el Convenio de Budapest y sus Protocolos Adicionales, quedan excluidos del régimen de infracciones administrativas de esta ley, siendo de aplicación exclusiva la vía penal. El CNCiber deberá efectuar la denuncia penal correspondiente cuando tome conocimiento de la presunta comisión de tales delitos, salvo que se trate de actividades amparadas por el artículo 21 bis° de la presente ley.

TÍTULO X — FINANCIAMIENTO

ARTÍCULO 31° — Recursos del CNCiber.

El Centro Nacional de Ciberseguridad (CNCiber) contará con los recursos necesarios para el cumplimiento de sus funciones, los cuales estarán integrados por:

a) Las partidas que le asigne la Ley de Presupuesto General de la Administración Nacional, las que deberán garantizar el adecuado funcionamiento del organismo conforme a sus competencias estratégicas y al carácter crítico de la ciberseguridad para la Nación.

b) Los fondos provenientes de convenios de cooperación técnica y financiera celebrados con organismos nacionales, internacionales o multilaterales, conforme la normativa vigente.

c) El producido de las multas aplicadas en ejercicio de sus competencias, el cual será destinado prioritariamente al fortalecimiento de capacidades operativas, tecnológicas y de respuesta ante incidentes.

d) Las donaciones, legados y aportes de terceros, los cuales deberán ser previamente evaluados en cuanto a su compatibilidad con los principios de independencia, transparencia y ausencia de conflictos de interés, conforme lo establezca la reglamentación.

e) Los bienes y recursos provenientes de decomisos o recupero de activos vinculados a delitos informáticos o a actividades ilícitas en el ciberespacio, conforme lo determine la autoridad judicial competente.

f) Los ingresos derivados de servicios de asistencia técnica, capacitación o certificación que el CNCiber brinde en el marco de sus competencias, conforme lo establezca la reglamentación.

g) Cualquier otro recurso que le sea asignado por la normativa vigente.

El CNCiber deberá administrar sus recursos con criterios de eficiencia, transparencia y rendición de cuentas, conforme a las disposiciones de la Ley N° 24.156 de Administración Financiera del Sector Público Nacional.

TÍTULO XI — DISPOSICIONES COMPLEMENTARIAS Y TRANSITORIAS

ARTÍCULO 32° — Reglamentación. El Poder Ejecutivo Nacional reglamentará la presente ley dentro del plazo de ciento ochenta (180) días corridos desde su promulgación. La reglamentación no podrá restringir los derechos reconocidos en la presente ley ni establecer condiciones que desnaturalicen su ejercicio efectivo.

ARTÍCULO 33° — Absorción de Organismos Preexistentes. Los organismos, unidades y programas que actualmente ejerzan competencias en materia de ciberseguridad en el ámbito de la Administración Pública Nacional y que hayan sido creados por decreto del Poder Ejecutivo serán absorbidos, fusionados o reorientados al CNCiber mediante decreto del Poder Ejecutivo Nacional dentro del plazo de ciento ochenta (180) días, garantizando la continuidad del personal y los derechos laborales adquiridos.

Respecto de los organismos creados por ley formal cuyas competencias en materia de ciberseguridad resulten alcanzadas por la presente norma, el Poder Ejecutivo Nacional remitirá al Honorable Congreso de la Nación, dentro del mismo plazo, los proyectos de ley de adecuación correspondientes. Hasta tanto dichas leyes sean sancionadas, tales organismos continuarán ejerciendo sus competencias en coordinación con el CNCiber.

ARTÍCULO 34° — Plazo de Adecuación. Los sujetos obligados del sector privado dispondrán de un plazo de ciento ochenta (180) días a partir de la publicación del reglamento de la presente ley para cumplir con las obligaciones del artículo 7°. Los operadores de infraestructuras críticas

dispondrán de trescientos sesenta (360) días para la plena adecuación a las obligaciones del artículo 16°. Los proveedores del Registro RNPTIC dispondrán de ciento ochenta (180) días desde su inscripción para cumplir con las obligaciones del artículo 21 ter°.

ARTÍCULO 35° — Adhesión Provincial. El Poder Ejecutivo Nacional, a través del CNCiber, invitará a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir a la presente ley y a los estándares mínimos que emita el CNCiber, mediante la suscripción de convenios de cooperación que contemplen la creación de CSIRTs provinciales y la integración a la Red Nacional de CSIRTs. El CNCiber priorizará la asistencia técnica a las provincias que adhieran.

ARTÍCULO 36° — Revisión Legislativa. El Congreso de la Nación realizará una revisión integral de la presente ley a los cuatro (4) años de su promulgación, con el objetivo de adecuarla al estado de la técnica, a la evolución del marco internacional y a la experiencia acumulada en su aplicación. El CNCiber elaborará un informe de evaluación que servirá de base para dicha revisión, el que será remitido a la Comisión Bicameral de Supervisión con antelación mínima de seis (6) meses al vencimiento del plazo.

ARTÍCULO 37° — Comunicación. Comuníquese al Poder Ejecutivo Nacional.

RAMIRO GUTIÉRREZ

DIPUTADO NACIONAL.-

FUNDAMENTOS.-

Sr. Presidente:

La República Argentina carece, a la fecha, de un marco legal integral, sistemático y coherente en materia de ciberseguridad. Las normas vigentes —Ley N° 25.326 de Protección de Datos Personales, Ley N° 26.388 de Delitos Informáticos y Ley N° 27.411 que aprueba el Convenio de Budapest— abordan aspectos parciales del fenómeno, sin establecer una arquitectura institucional coordinada, ni obligaciones generales de prevención, gestión de riesgos y respuesta ante incidentes para los actores críticos del ecosistema digital.

Asimismo, las capacidades estatales existentes en la materia —como la Dirección Nacional de Ciberseguridad creada por el Decreto N° 1.082/2019— carecen de jerarquía legal suficiente, autonomía funcional y herramientas normativas adecuadas para ejercer una rectoría efectiva a nivel nacional.

Esta debilidad normativa se traduce en consecuencias concretas. En los últimos años, la Argentina ha sufrido incidentes de alta criticidad que afectaron organismos públicos y sistemas esenciales, tales como el ataque a la Dirección Nacional de Migraciones (2020), la vulneración del sistema del Poder Judicial de Córdoba (2022), el acceso indebido a bases de datos del RENAPER (2021) y múltiples incidentes en el sistema de salud. En estos casos, la ausencia de un marco legal integral impidió establecer obligaciones claras de prevención, notificación, respuesta coordinada y rendición de cuentas.

El presente proyecto tiene por objeto subsanar estas deficiencias mediante la creación de un **Sistema Nacional de Ciberseguridad**, estructurado en torno a una autoridad rectora —el Centro Nacional de Ciberseguridad (CNCiber)— con competencias de coordinación, regulación técnica y

articulación interinstitucional, respetando estrictamente el reparto de funciones previsto en las Leyes N° 23.554 de Defensa Nacional, 24.059 de Seguridad Interior y 25.520 de Inteligencia Nacional.

Asimismo, el proyecto incorpora como instrumento central la **Estrategia Nacional de Ciberseguridad (artículo 13)**, concebida como la herramienta de planificación estratégica que permitirá ordenar, priorizar y dar coherencia a la acción estatal en la materia. La ausencia histórica de una estrategia formal ha derivado en respuestas fragmentadas, reactivas y desarticuladas frente a incidentes cibernéticos.

La institucionalización de una Estrategia Nacional, con horizonte plurianual, revisión periódica e indicadores medibles, permitirá identificar amenazas prioritarias, definir roles y responsabilidades entre los distintos organismos del Estado, y orientar la asignación eficiente de recursos públicos. Asimismo, posibilitará integrar de manera coherente las dimensiones de ciberseguridad, ciberdefensa y política exterior, fortaleciendo la posición de la Argentina en los foros internacionales y en los esquemas de cooperación regional.

En este sentido, la Estrategia Nacional no constituye una mera declaración programática, sino un verdadero instrumento de gobernanza que articula al sector público, al sector privado, a la academia y a la sociedad civil, consolidando un enfoque integral, preventivo y basado en la gestión de riesgos.

El diseño institucional adoptado incorpora **límites explícitos al ejercicio de las funciones del CNCiber**, estableciendo que el organismo no podrá ejercer tareas de inteligencia, investigación criminal ni funciones propias de las fuerzas de seguridad, garantizando así la separación funcional y evitando superposiciones indebidas.

Asimismo, el proyecto establece **garantías robustas en materia de derechos fundamentales**, disponiendo que toda actividad de monitoreo sobre redes privadas requerirá autorización judicial previa o consentimiento válido del titular, y prohibiendo de manera expresa la vigilancia masiva, indiscriminada o no focalizada. Estas previsiones se ven

reforzadas por la exigencia de registro de las actividades de monitoreo y su sometimiento a control institucional.

En este sentido, una de las innovaciones centrales del proyecto es la creación de la **Comisión Bicameral de Supervisión de la Ciberseguridad Nacional (artículo 12 bis)**, que introduce un mecanismo de control parlamentario permanente sobre el funcionamiento del sistema. Este órgano permite dotar de efectividad a las garantías establecidas, asegurando supervisión democrática, acceso a información relevante —incluyendo aquella de carácter clasificado— y capacidad de seguimiento de las políticas públicas en la materia.

El proyecto también incorpora un **régimen integral de gestión de riesgos y obligaciones de ciberseguridad** para los sujetos obligados, en particular los operadores de infraestructuras críticas y proveedores digitales esenciales, estableciendo estándares mínimos, deberes de notificación de incidentes y exigencias de continuidad operativa. Este enfoque preventivo y sistémico resulta indispensable frente a un entorno de amenazas crecientemente complejo.

En línea con las mejores prácticas internacionales, se introduce el **régimen de divulgación coordinada de vulnerabilidades (artículo 21 bis)**, que otorga certeza jurídica a los investigadores de seguridad que actúan de buena fe. El proyecto establece expresamente una exención condicionada de responsabilidad penal y civil para aquellas conductas estrictamente necesarias para la identificación y reporte de vulnerabilidades, siempre que se cumplan requisitos estrictos. De este modo, se alinean los incentivos para fomentar la detección temprana de fallas de seguridad sin criminalizar conductas socialmente valiosas.

Asimismo, se incorpora un **régimen de seguridad de la cadena de suministro tecnológica del Estado (artículo 21 ter)**, incluyendo la obligación de utilización de Listas de Materiales de Software (SBOM). Esta previsión responde a uno de los vectores de ataque más críticos a nivel global, permitiendo identificar dependencias, vulnerabilidades y riesgos asociados al software utilizado en sistemas estatales.

El proyecto también prevé un **régimen sancionatorio proporcional y diferenciado**, que contempla tanto al sector privado como a los organismos públicos, incorporando mecanismos de publicidad de incumplimientos, responsabilidad jerárquica y control parlamentario. Este esquema busca alinear incentivos, promoviendo el cumplimiento efectivo de las obligaciones sin desnaturalizar la función pública.

En materia federal, la iniciativa respeta plenamente la distribución constitucional de competencias, estableciendo obligaciones sobre sujetos de jurisdicción nacional o de impacto interjurisdiccional, e invitando a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir voluntariamente a los estándares establecidos, mediante mecanismos de cooperación.

El proyecto recepta los principales estándares y marcos internacionales, entre ellos el NIST Cybersecurity Framework 2.0 (2024), la Directiva NIS2 de la Unión Europea, el Convenio de Budapest y su Segundo Protocolo Adicional, así como experiencias comparadas relevantes en la región, como la legislación chilena reciente en la materia y el desarrollo normativo brasileño.

En definitiva, la presente iniciativa propone un equilibrio adecuado entre **eficacia en la protección del ciberespacio nacional y resguardo de los derechos fundamentales**, estableciendo un sistema moderno, transparente, controlado democráticamente y alineado con los estándares internacionales.

Por los motivos expuestos, solicitamos la aprobación del presente proyecto de ley.