DIPUTADOS
ARGENTINA

PROYECTO DE LEY

EL SENADO Y LA CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA
REUNIDOS EN CONGRESO SANCIONAN CON FUERZA DE LEY:

LEY DE NEUROSEGURIDAD

Y CIBERSEGURIDAD DE DISPOSITIVOS

MÉDICOS CONECTADOS

TÍTULO I – DISPOSICIONES GENERALES

ARTÍCULO 1º — *Objeto.*

La presente ley tiene por objeto establecer el régimen de ciberseguridad específico para dispositivos médicos conectados y neurotecnologías, a fin de proteger la vida, la integridad física y psíquica, la privacidad y la seguridad de los pacientes y usuarios frente a los riesgos de ciberseguridad inherentes a la conectividad, la actualización remota de software y el procesamiento de datos de salud y neurodatos por dichos dispositivos.

ARTÍCULO 2º — *Ámbito de aplicación.*

La presente ley se aplica a:

a) Todo dispositivo médico conforme la definición de la ANMAT que incluya software, conectividad a internet o redes, capacidad de actualización remota, o intercambio electrónico de datos de salud (dispositivo médico conectado).

b) Todo software utilizado como dispositivo médico (Software as a Medical Device, SaMD), incluyendo aplicaciones móviles con función médica regulada.

c) Toda neurotecnología conforme la definición establecida por la normativa aplicable en materia de neuroderechos, ya sea de uso terapéutico, de investigación, recreativo o de consumo, que interaccione con el sistema nervioso.

d) Los sistemas y componentes asociados al funcionamiento de los dispositivos comprendidos en los incisos anteriores, incluyendo servidores de actualización,

plataformas en la nube, módulos de conectividad, programadores clínicos y aplicaciones de monitoreo remoto.

Quedan exceptuados los dispositivos médicos que no contengan software ni capacidad de conectividad.

ARTÍCULO 3º — *Definiciones.*

A los efectos de la presente ley se entiende por:

a) Dispositivo médico conectado (DMC): Todo dispositivo médico que incluya software, se conecte a internet, redes locales u otros dispositivos, reciba actualizaciones remotas o intercambie datos electrónicamente.

b) Neurodispositivo: Neurotecnología que interactúa directa o indirectamente con el sistema nervioso central o periférico de una persona, ya sea invasiva (implantes neurales, interfaces cerebro-computadora invasivas) o no invasiva (EEG portátil, estimulación transcraneal, neurofeedback).

c) Neurodispositivo crítico: Neurodispositivo invasivo cuya falla o compromiso de seguridad pueda causar la muerte, daño físico grave o alteración irreversible de la actividad neuronal del paciente.

d) Cibervulnerabilidad: Debilidad en el diseño, implementación, operación o configuración de un DMC o neurodispositivo que pueda ser explotada por una amenaza para comprometer la seguridad, integridad, disponibilidad o confidencialidad del dispositivo o de los datos que procesa.

e) Incidente de neuroseguridad: Todo evento que comprometa o amenace la seguridad, integridad, disponibilidad o confidencialidad de un DMC o neurodispositivo, o de los datos de salud o neurodatos que procesa, incluyendo accesos no autorizados, alteraciones de funcionamiento, inyección de código malicioso e interceptación de datos.

f) SBOM (Software Bill of Materials): Inventario detallado y estructurado de todos los componentes de software, bibliotecas, módulos y dependencias que integran el software de un DMC o neurodispositivo.

g) Ciclo de vida de ciberseguridad: Proceso continuo de gestión de la ciberseguridad del dispositivo desde su diseño hasta su retiro del mercado, incluyendo diseño seguro, pruebas, despliegue, monitoreo, actualización, respuesta a incidentes y descomisionamiento.

h) Actualización de seguridad: Modificación del software de un DMC o neurodispositivo destinada a corregir cibervulnerabilidades o mejorar la seguridad, distinguiéndose de las

actualizaciones funcionales que modifican las prestaciones del dispositivo.

i) Fin de soporte de seguridad: Fecha a partir de la cual el fabricante cesa de proporcionar actualizaciones de seguridad para un DMC o neurodispositivo.

TÍTULO II – CLASIFICACIÓN POR NIVEL DE RIESGO DE CIBERSEGURIDAD

ARTÍCULO 4º — *Niveles de riesgo.*

Los DMC y neurodispositivos se clasifican en los siguientes niveles de riesgo de ciberseguridad:

a) Nivel 1 — Riesgo bajo: Dispositivos sin conectividad de red directa, con funciones de software limitadas y cuyo compromiso no puede afectar la seguridad del paciente. Ejemplo: software de gestión administrativa de clínicas.

b) Nivel 2 — Riesgo moderado: DMC con conectividad de red que procesan datos de salud pero cuyo compromiso no puede afectar directamente la seguridad física del paciente. Ejemplo: plataformas de monitoreo remoto de signos vitales, aplicaciones de salud mental.

c) Nivel 3 — Riesgo alto: DMC cuyo compromiso puede afectar la seguridad física del paciente o la integridad de diagnósticos clínicos. Ejemplo: bombas de infusión conectadas, sistemas de cirugía robótica, dispositivos cardíacos implantables con conectividad, neurodispositivos no invasivos de uso terapéutico.

d) Nivel 4 — Riesgo crítico: Neurodispositivos críticos cuyo compromiso puede causar la muerte, daño físico grave o alteración irreversible de la actividad neuronal. Ejemplo: implantes neurales, interfaces cerebro-computadora invasivas, estimuladores cerebrales profundos conectados.

La ANMAT, en coordinación con la ANPDP, clasificará los dispositivos conforme estos niveles y actualizará la clasificación con periodicidad anual.

TÍTULO III – OBLIGACIONES DE LOS FABRICANTES

Capítulo 1 – Seguridad por diseño

ARTÍCULO 5º — *Principio de seguridad por diseño.*

Todo fabricante de DMC o neurodispositivo deberá integrar la ciberseguridad como componente esencial del diseño del dispositivo, no como adición posterior. La ciberseguridad deberá ser considerada en cada etapa del proceso de desarrollo, desde

la concepción hasta el retiro del mercado, conforme el principio de ciclo de vida de ciberseguridad.

ARTÍCULO 6º — *Requisitos técnicos mínimos.*

Todo DMC y neurodispositivo deberá cumplir, como mínimo, los siguientes requisitos técnicos de ciberseguridad, graduados según su nivel de riesgo:

a) Autenticación y control de acceso: Mecanismos de autenticación robustos para todo acceso al dispositivo, sus interfaces y sus datos. Para Nivel 3 y 4: autenticación multifactor obligatoria para accesos remotos.

b) Cifrado: Cifrado de datos en tránsito y en reposo conforme estándares criptográficos reconocidos. Para neurodispositivos: cifrado de extremo a extremo de neurodatos.

c) Integridad del software: Mecanismos de verificación de integridad que impidan la ejecución de código no autorizado o alterado. Firma digital de actualizaciones de software.

d) Registro de eventos (logging): Generación automática de registros de eventos de seguridad, incluyendo accesos, modificaciones, actualizaciones y anomalías, conservados por un mínimo de cinco (5) años.

e) Segmentación: Aislamiento lógico de las funciones críticas del dispositivo respecto de funciones no esenciales y de redes externas.

f) Resiliencia: Capacidad del dispositivo de continuar operando de manera segura ante la pérdida de conectividad o ante un ataque, mediante modos de operación degradados que preserven las funciones críticas de seguridad del paciente.

g) SBOM: Mantenimiento y actualización de un inventario completo de componentes de software (SBOM) en formato estandarizado, que será entregado a la ANMAT y puesto a disposición de las instituciones de salud que utilicen el dispositivo.

La ANMAT publicará estándares técnicos detallados para cada nivel de riesgo, alineados con los estándares internacionales (FDA, EU MDR/MDCG, IEC 62443, IEEE/UL 2933) y los actualizará bienalmente.

Capítulo 2 – Actualizaciones y soporte

ARTÍCULO 7º — *Obligación de actualización de seguridad.*

El fabricante deberá proporcionar actualizaciones de seguridad durante toda la vida útil del dispositivo, conforme los siguientes plazos mínimos:

a) Nivel 1 y 2: Mínimo cinco (5) años desde la última venta del dispositivo.

b) Nivel 3: Mínimo diez (10) años desde la última venta.

c) Nivel 4 (neurodispositivos críticos): Mínimo quince (15) años desde la última implantación, o la vida útil del dispositivo implantado, lo que resulte mayor.

Las actualizaciones de seguridad deberán ser provistas de manera gratuita. Las actualizaciones críticas deberán desplegarse dentro de las cuarenta y ocho (48) horas de descubierta la vulnerabilidad para Nivel 4, y dentro de los quince (15) días para Nivel 3.

ARTÍCULO 8º — *Fin de soporte y obsolescencia planificada.*

El fabricante deberá informar la fecha prevista de fin de soporte de seguridad al momento de la comercialización del dispositivo. La fecha deberá constar en el etiquetado, el manual de uso y el registro sanitario.

Con al menos veinticuatro (24) meses de anticipación al fin de soporte, el fabricante deberá notificar a las instituciones de salud, a la ANMAT y a los pacientes (cuando el dispositivo sea de uso domiciliario o implantado) sobre la fecha de fin de soporte y las alternativas disponibles.

Para neurodispositivos críticos implantados: el fin de soporte no podrá producirse mientras el dispositivo se encuentre implantado en un paciente, salvo que se proporcione un plan de transición aprobado por la ANMAT que garantice la seguridad del paciente, incluyendo cuando sea necesario la cobertura del costo de reemplazo del dispositivo.

Capítulo 3 – Notificación de incidentes y vulnerabilidades

ARTÍCULO 9º — *Notificación obligatoria de incidentes.*

El fabricante deberá notificar todo incidente de neuroseguridad a la ANMAT y, cuando involucre datos personales, a la ANPDP, conforme los siguientes plazos:

a) Nivel 4: Dentro de las seis (6) horas de que el fabricante haya tomado conocimiento razonable del incidente, entendido como el momento en que la información disponible permite concluir con grado razonable de certeza que se ha producido un compromiso de seguridad. La notificación inicial podrá ser provisoria y completarse dentro de las veinticuatro (24) horas siguientes con información detallada.

b) Nivel 3: Dentro de las veinticuatro (24) horas.

c) Nivel 2: Dentro de las setenta y dos (72) horas.

La notificación incluirá: descripción del incidente; dispositivos y pacientes afectados o potencialmente afectados; evaluación de riesgo; medidas adoptadas y previstas; y cronograma de remediación.

Cuando el incidente represente un riesgo inminente para la vida o la integridad física de pacientes, el fabricante deberá notificar telefónicamente a la ANMAT de manera inmediata, sin perjuicio de la notificación formal.

ARTÍCULO 10º — *Divulgación coordinada de vulnerabilidades.*

El fabricante deberá establecer un mecanismo público y accesible para que investigadores de seguridad, profesionales de la salud y cualquier persona puedan reportar cibervulnerabilidades de manera confidencial.

El fabricante no podrá emprender acciones legales contra investigadores de seguridad que reporten vulnerabilidades de buena fe y conforme las prácticas de divulgación coordinada (responsible disclosure). Se considerará divulgación coordinada la comunicación al fabricante con un plazo razonable para la remediación antes de la divulgación pública.

La ANMAT mantendrá un portal público de alertas de seguridad de dispositivos médicos conectados, actualizado con la información de vulnerabilidades confirmadas y medidas de mitigación.

TÍTULO IV – OBLIGACIONES DE LAS INSTITUCIONES DE SALUD

ARTÍCULO 11º — *Gestión de ciberseguridad institucional.*

Toda institución de salud que utilice DMC o neurodispositivos deberá:

a) Mantener un inventario actualizado de todos los DMC y neurodispositivos en operación, incluyendo versión de software, estado de actualización y fecha de fin de soporte.

b) Implementar las actualizaciones de seguridad provistas por el fabricante dentro de los plazos que establezca la reglamentación.

c) Segmentar las redes hospitalarias para aislar los DMC críticos de las redes administrativas y de acceso público.

d) Designar un responsable de ciberseguridad de dispositivos médicos, que podrá ser el mismo oficial de seguridad informática de la institución.

e) Capacitar al personal clínico en buenas prácticas de ciberseguridad de dispositivos

médicos.

f) Elaborar y mantener actualizado un plan de respuesta a incidentes de ciberseguridad específico para DMC y neurodispositivos.

ARTÍCULO 12º — *Dispositivos obsoletos.*

Las instituciones de salud no podrán mantener en operación DMC o neurodispositivos cuyo soporte de seguridad haya finalizado, salvo que: a) el dispositivo esté físicamente aislado de toda red, sin capacidad de comunicación; b) se haya implementado un plan de mitigación de riesgos aprobado por el responsable de ciberseguridad; y c) se notifique a la ANMAT la continuación del uso y las medidas adoptadas. Para neurodispositivos críticos implantados sin soporte, se aplicará el plan de transición del artículo 8.

TÍTULO V – PROTECCIÓN ESPECIAL DE NEURODISPOSITIVOS

ARTÍCULO 13º — *Régimen reforzado para neurodispositivos críticos.*

Además de las obligaciones generales, los neurodispositivos críticos (Nivel 4) estarán sujetos a:

a) Certificación de ciberseguridad obligatoria: Evaluación de ciberseguridad realizada por un organismo certificador acreditado por la ANMAT, como requisito previo al registro sanitario y la comercialización.

b) Pruebas de penetración (pentesting): Realización de pruebas de penetración por terceros independientes antes de la comercialización y con periodicidad anual durante toda la vida útil del dispositivo.

c) Mecanismo de desactivación de emergencia: Todo neurodispositivo crítico implantado deberá contar con un mecanismo físico o lógico seguro de desactivación de emergencia accesible al equipo médico, que permita interrumpir el funcionamiento del dispositivo ante un compromiso de seguridad sin requerir cirugía.

d) Criptografía de largo plazo: Los neurodispositivos críticos cuya vida útil prevista supere los diez (10) años deberán implementar algoritmos de cifrado aprobados por organismos de estandarización internacionales reconocidos (NIST, ISO/IEC) que sean resistentes a las amenazas conocidas y previsibles al momento de la comercialización, incluyendo la amenaza de computación cuántica cuando existan estándares aprobados. Cuando no existan estándares post-cuánticos plenamente aprobados al momento de la comercialización, el fabricante deberá presentar un plan de transición criptográfica que prevea la actualización de los algoritmos de cifrado del dispositivo sin requerir

intervención quirúrgica ni reemplazo del hardware, dentro de los doce (12) meses de la aprobación de dichos estándares.

e) Protección de neurodatos en dispositivo: Los neurodatos procesados por el dispositivo deberán cifrarse localmente antes de cualquier transmisión, y el paciente tendrá derecho a conocer y controlar qué neurodatos son transmitidos fuera del dispositivo.

ARTÍCULO 14º — *Consentimiento informado de ciberseguridad.*

Previo a la implantación o primera utilización de un neurodispositivo, el paciente deberá recibir información específica sobre:

a) Los riesgos de ciberseguridad del dispositivo, en lenguaje comprensible.

b) Las medidas de seguridad implementadas y sus limitaciones.

c) La política de actualizaciones de seguridad y la fecha prevista de fin de soporte.

d) Los tipos de datos (incluyendo neurodatos) que el dispositivo recolecta, procesa y transmite.

e) Los derechos del paciente respecto de sus datos conforme la normativa aplicable en materia de protección integral de datos personales y de neuroderechos.

f) El mecanismo de desactivación de emergencia, cuando aplique.

Este consentimiento es adicional al consentimiento médico informado requerido por la Ley Nº 26.529 de Derechos del Paciente.

TÍTULO VI – AUTORIDAD DE APLICACIÓN Y RÉGIMEN SANCIONATORIO

ARTÍCULO 15º — *Autoridad de Aplicación.*

Será Autoridad de Aplicación la Administración Nacional de Medicamentos, Alimentos y Tecnología Médica (ANMAT), en coordinación con la Autoridad Nacional de Protección de Datos Personales (ANPDP) para las materias de protección de datos y neurodatos, y con la Dirección Nacional de Ciberseguridad o el organismo que la reemplace para las materias de seguridad informática.

La ANMAT creará una Unidad de Ciberseguridad de Dispositivos Médicos, dotada de profesionales en seguridad informática, ingeniería biomédica y regulación sanitaria, con presupuesto operativo diferenciado.

Para el ejercicio de sus funciones de evaluación, certificación y auditoría de

ciberseguridad, la ANMAT implementará un modelo mixto:

a) Funciones soberanas indelegables: clasificación de riesgo, registro sanitario, gestión de incidentes críticos, órdenes de retiro y suspensión.

b) Funciones delegables a terceros acreditados: evaluaciones de ciberseguridad, certificación de neurodispositivos, pruebas de penetración, auditorías de SBOM y evaluaciones de conformidad técnica.

La ANMAT establecerá un régimen de acreditación de organismos certificadores de ciberseguridad de dispositivos médicos, que incluirá requisitos de independencia, competencia técnica demostrable, seguro de responsabilidad profesional, y auditoría periódica de la ANMAT sobre los certificadores acreditados.

La ANMAT podrá celebrar convenios con universidades nacionales, el CONICET y organismos internacionales de regulación sanitaria (FDA, EMA, IMDRF) para asistencia técnica y reconocimiento recíproco de certificaciones.

ARTÍCULO 16º — *Funciones de la Autoridad.*

Son funciones de la Autoridad de Aplicación:

a) Clasificar los DMC y neurodispositivos por nivel de riesgo de ciberseguridad.

b) Publicar y actualizar estándares técnicos de ciberseguridad por nivel de riesgo.

c) Evaluar la ciberseguridad como componente del registro sanitario.

d) Acreditar organismos certificadores de ciberseguridad de neurodispositivos.

e) Recibir y gestionar notificaciones de incidentes y vulnerabilidades.

f) Mantener el portal público de alertas de seguridad.

g) Ordenar retiros del mercado, suspensiones o restricciones de uso por motivos de ciberseguridad.

h) Coordinar con la ANPDP la protección de datos de salud y neurodatos en dispositivos.

i) Cooperar internacionalmente con agencias regulatorias de dispositivos médicos (FDA, EMA, autoridades EU MDR, IMDRF) en materia de ciberseguridad.

ARTÍCULO 17º — *Infracciones y sanciones.*

Las infracciones se clasifican en:

a) Leves: Incumplimiento de obligaciones formales de etiquetado, documentación de SBOM o registro de eventos. Sanción: apercibimiento y/o multa de hasta quinientos

(500) SMVM.

b) Graves: Comercialización sin cumplir requisitos técnicos mínimos; omisión de actualizaciones de seguridad; incumplimiento de notificación de incidentes; continuación de soporte sin notificación de fin de vida. Sanción: multa de hasta cinco mil (5.000) SMVM; suspensión del registro sanitario hasta cumplimiento.

c) Muy graves: Comercialización de neurodispositivos críticos sin certificación de ciberseguridad; ocultamiento de vulnerabilidades conocidas; acciones legales contra investigadores de buena fe; abandono de soporte de neurodispositivo crítico implantado sin plan de transición. Sanción: multa de hasta veinte mil (20.000) SMVM; revocación del registro sanitario; inhabilitación para comercializar dispositivos por hasta diez (10) años. La graduación de las sanciones atenderá especialmente al impacto real o potencial en la seguridad de los pacientes, la gravedad y extensión de la vulnerabilidad, la diligencia demostrada en la respuesta al incidente, la cooperación con las autoridades, y la existencia de un seguro de ciberseguridad vigente. Se reconoce el crédito de cumplimiento: los fabricantes que acrediten certificación de ciberseguridad vigente, seguro de responsabilidad por ciberincidentes, programa de divulgación coordinada de vulnerabilidades, y auditoría de penetración anual, gozarán de una reducción de hasta el cuarenta por ciento (40%) en la sanción, sin poder bajar del mínimo de la categoría. Adicionalmente, la ANMAT, en coordinación con la Superintendencia de Seguros de la Nación, promoverá que las primas de seguro de responsabilidad por ciberincidentes de dispositivos médicos se gradúen conforme el nivel de cumplimiento de los requisitos de la presente ley, generando incentivos de mercado complementarios al régimen sancionatorio.

Las sanciones son sin perjuicio de las responsabilidades civiles conforme la normativa aplicable en materia de responsabilidad civil por daños de sistemas de inteligencia artificial y el Código Civil y Comercial de la Nación, y de las responsabilidades penales que correspondan.

TÍTULO VII – DISPOSICIONES COMPLEMENTARIAS Y TRANSITORIAS

ARTÍCULO 18º — *Coordinación normativa.*

La presente ley se aplicará complementaria y coordinadamente con la normativa que regule los neuroderechos, la protección integral de datos personales, la responsabilidad civil por daños de sistemas de inteligencia artificial, los datos biométricos, la evaluación de impacto algorítmico, los derechos digitales de niñas, niños y adolescentes, la Ley Nº 26.529 de Derechos del Paciente, y toda normativa de la ANMAT aplicable a dispositivos médicos. En caso de conflicto, prevalecerá la norma que otorgue mayor protección a la

seguridad del paciente.

ARTÍCULO 19º — *Cláusula pro-innovación.*

La presente ley promueve el desarrollo de dispositivos médicos conectados y neurotecnologías seguros. La ANMAT podrá establecer un sandbox regulatorio de ciberseguridad que permita probar dispositivos innovadores bajo condiciones controladas, con monitoreo reforzado y sin exención de los requisitos de seguridad del paciente. El sandbox tendrá una duración de hasta veinticuatro (24) meses prorrogables, admitirá hasta quince (15) proyectos simultáneos y priorizará desarrollos con potencial de impacto en salud pública, enfermedades raras o neurotecnologías de rehabilitación. Se establece un régimen de compliance progresivo para fabricantes nacionales con facturación inferior a la categoría de pequeña empresa: a) durante los primeros tres (3) años de comercialización, podrán cumplir los requisitos técnicos del artículo 6 conforme un plan de adecuación progresiva aprobado por la ANMAT, que establezca hitos verificables de cumplimiento; b) podrán utilizar certificadores acreditados con tarifas diferenciadas que la ANMAT establecerá; c) tendrán acceso prioritario al sandbox y a los programas de asistencia técnica. En ningún caso el régimen progresivo podrá reducir los requisitos de seguridad del paciente para dispositivos de Nivel 3 o 4. Se promoverá la cooperación con universidades nacionales y el CONICET para la investigación en ciberseguridad de dispositivos médicos y neurotecnologías.

ARTÍCULO 20º — *Plazo de adecuación.*

Los fabricantes e instituciones de salud dispondrán de los siguientes plazos desde la reglamentación:

a) Doce (12) meses para el cumplimiento de los requisitos de notificación de incidentes y mantenimiento de SBOM.

b) Veinticuatro (24) meses para el cumplimiento integral de los requisitos técnicos mínimos del artículo 6.

c) Treinta y seis (36) meses para la certificación de ciberseguridad de neurodispositivos críticos ya comercializados.

Los dispositivos nuevos comercializados después de la entrada en vigencia deberán cumplir desde su lanzamiento.

ARTÍCULO 21º — *Reglamentación.*

El Poder Ejecutivo Nacional reglamentará la presente ley dentro de los ciento ochenta

(180) días de su publicación, con intervención de la ANMAT, la ANPDP y la Dirección Nacional de Ciberseguridad.

ARTÍCULO 22º — *Vigencia.*

La presente ley entrará en vigencia a los noventa (90) días de su publicación.

ARTÍCULO 23º — *Comunicación.*

Comuníquese al Poder Ejecutivo Nacional.

LIC. MARCELA MARINA PAGANO
DIPUTADA DE LA NACIÓN

DIPUTADOS
ARGENTINA

FUNDAMENTOS

Señor Presidente:

I. El problema. Un implante neural hackeado no es un problema de privacidad: es un problema de integridad física. Una bomba de infusión comprometida puede matar. Un estimulador cerebral profundo alterado remotamente puede causar daño neurológico irreversible. La convergencia entre dispositivos médicos, conectividad y neurotecnología ha creado una superficie de ataque sin precedentes que la regulación sanitaria tradicional no contempla. La FDA reportó aproximadamente 950 dispositivos médicos con IA/ML autorizados a mediados de 2024, con unas 100 nuevas aprobaciones anuales. Neuralink realizó su primer implante en humanos en enero de 2024. El mercado de dispositivos médicos con IA se estima en 13.700 millones de dólares en 2024, proyectándose a 255.000 millones para 2033.

II. La brecha argentina. La Argentina implementó en 2024 una nueva resolución de dispositivos médicos (237/2024) que incluye vigilancia post-mercado, pero carece de un régimen específico de ciberseguridad para dispositivos conectados y neurotecnologías. La Ley Nacional de Neuroderechos que este Congreso impulsa protege la integridad mental y los neurodatos, pero no regula la seguridad técnica de los dispositivos que interactúan con el cerebro. Esta ley cierra esa brecha.

III. El contexto internacional. La FDA publicó en junio de 2025 su guía final de ciberseguridad de dispositivos médicos, expandiendo la definición de “cyber device” y estableciendo obligaciones de ciclo de vida completo. La UE adoptó el Cyber Resilience Act (2024/2847) con requisitos horizontales de ciberseguridad y propuso reforzar el MDR con obligaciones específicas, incluyendo reporte de vulnerabilidades activamente explotadas. El IMDRF (International Medical Device Regulators Forum) trabaja en una guía global armonizada de ciberseguridad. Este proyecto se alinea con estos estándares y los supera en la protección específica de neurodispositivos.

IV. Innovaciones del proyecto. Cinco aspectos distinguen esta ley. Primero, la clasificación en cuatro niveles de riesgo de ciberseguridad con un nivel específico para neurodispositivos críticos, inexistente en cualquier otra jurisdicción. Segundo, la obligación de soporte de seguridad durante quince años para neurodispositivos implantados, con prohibición de abandonar el soporte mientras el dispositivo esté implantado. Tercero, la exigencia de cifrado resistente a computación cuántica para dispositivos de larga vida útil, anticipando la amenaza post-cuántica. Cuarto, el mecanismo de desactivación de emergencia para implantes neurales, que garantiza que un equipo médico pueda interrumpir un dispositivo comprometido sin cirugía. Quinto, la protección legal de investigadores de seguridad que reporten vulnerabilidades de

buena fe, alineada con las mejores prácticas internacionales de responsible disclosure.

V. Integración sistémica. Esta es la octava y última pieza del Sistema Argentino de Gobernanza de IA. Cierra el ciclo: la Ley de Neuroderechos protege la integridad mental; la de Datos Personales protege los neurodatos; la de Responsabilidad Civil repara los daños; la de Biométricos regula la identificación; la de Evaluación de Impacto previene riesgos; la de Derechos Digitales de NNA protege a menores; y esta ley garantiza que los dispositivos que interactúan con el cuerpo y el cerebro sean seguros. Juntas, constituyen el marco regulatorio integrado más completo del mundo en materia de protección de la persona en el entorno digital y neurotecnológico.

Por todo lo expuesto, solicito a mis pares la aprobación del presente proyecto de ley.

LIC. MARCELA MARINA PAGANO
DIPUTADA DE LA NACIÓN