ANEXO TEMÁTICO · SOBERANÍA DIGITAL EN ARGENTINA

LITAT

Ciberseguridad y soberanía digital.

Anexo temático al documento "Soberanía digital en Argentina" (LITAT). ¿Puede Argentina ejercer soberanía digital si el Estado no tiene una arquitectura propia y coordinada para conocer sus activos digitales, protegerlos, detectar agresiones, responder a incidentes, recuperar sus servicios y aprender de las crisis?

DOCUMENTO
Anexo temático · LITAT

AFIRMACIONES CENTRALES
5 (AC1 a AC5)

RECOMENDACIONES
8 líneas de acción (R1 a R8)

TIEMPO DE LECTURA
~25 minutos

01 · MARCO

La ciberseguridad como condición de la soberanía digital.

La soberanía digital no se ejerce solamente decidiendo dónde residen los datos o quién es propietario de la infraestructura: se ejerce, ante todo, teniendo la capacidad de **proteger, conocer y sostener en el tiempo** los sistemas de los que depende el funcionamiento del Estado, la economía y la vida cotidiana de las personas.

Sin esa capacidad, cualquier otra dimensión de la soberanía digital (propiedad de la infraestructura, control de los datos, autonomía productiva) queda expuesta a interrupciones, filtraciones o manipulaciones que ningún marco jurídico puede prevenir por sí solo.

Esta no es una preocupación exclusivamente argentina. El Índice Global de Ciberseguridad 2024 de la Unión Internacional de Telecomunicaciones[1] ubica a la Argentina en un nivel intermedio de desarrollo ("Tier 4", sobre 194 países evaluados), por debajo de Brasil y Estados Unidos en la región. El Banco Interamericano de Desarrollo y la Organización de los Estados Americanos coinciden en que la madurez regional mejoró entre 2020 y 2025, sin discriminar resultados por país[2]. La CEPAL[3], por su parte, documenta un aumento de incidentes y una disparidad normativa considerable entre los países de la región. Argentina, además, es parte del Convenio de Budapest sobre Ciberdelito desde su entrada en vigor para el país el 1° de octubre de 2018, tras su aprobación por Ley 27.411 (2017) y ratificación en junio de 2018 (el tratado internacional entró en vigor a nivel general en 2004, pero la adhesión argentina es posterior), junto con otros diez países de América Latina y el Caribe.

Tier 4
Nivel de la Argentina en el Índice Global de Ciberseguridad 2024 (UIT)

188
Países evaluados en el índice

2018
Entrada en vigor del Convenio de Budapest para la Argentina (Ley 27.411)

La segunda estrategia nacional de ciberseguridad, publicada por resolución ministerial en 2023[4], la define como el:

> **“Conjunto de políticas y acciones orientadas a elevar los niveles de seguridad de las infraestructuras de las TIC, que podrían, según el caso, ser potencialmente vulnerables ante amenazas y/o incidentes. De este modo, se tiene como objetivo prevenir acciones que afecten la administración del Estado, las organizaciones, los servicios esenciales y, en consecuencia, a las personas”.**

Definida así, consideramos que la ciberseguridad no se agota en la prevención de ataques. Es una capacidad continua para **gobernar, conocer, proteger, detectar, responder, recuperar y aprender** frente a los riesgos digitales.

LA PREGUNTA DE ESTE CAPÍTULO

¿Puede Argentina ejercer soberanía digital si el Estado no tiene arquitectura propia y coordinada para conocer sus activos digitales, protegerlos, detectar agresiones, responder a incidentes, recuperar sus servicios y aprender de las crisis, **ya sea porque esas funciones están dispersas entre organismos que no se coordinan entre sí, ya sea porque dependen de terceros externos que el Estado no controla?**

02 · AFIRMACIONES

Afirmaciones centrales.

Validadas contra la matriz de trazabilidad (de normas, estructuras y publicaciones), sostienen tanto el diagnóstico como las recomendaciones.

AC1 MARCO CONCEPTUAL DEL TRABAJO

La ciberseguridad no es un capítulo técnico accesorio sino una condición operativa de la soberanía digital: sin capacidad de conocer, proteger, detectar, responder, recuperar y aprender, la soberanía sobre infraestructura, datos y algoritmos que reclaman los capítulos anteriores no es sostenible ante una brecha real.

AC2 DIAGNÓSTICO PRINCIPAL

Argentina ha multiplicado organismos con competencia en la materia en los últimos veinte meses (circuito policial-criminal, circuito de ciberinteligencia bajo la SIDE, circuito técnico-regulatorio del CNC) sin que ninguna norma de rango superior establezca protocolos de deslinde entre ellos.

AC3 DIAGNÓSTICO FORMULADO CON CAUTELA · MENOR DENSIDAD DE EVIDENCIA

Buena parte de la capacidad de detección, protección y respuesta del Estado y de los operadores de infraestructura crítica argentinos depende de proveedores, plataformas e infraestructura no nacionales, lo cual, siguiendo el propio marco del documento madre, no equivale automáticamente a vulnerabilidad, pero sí exige capacidad de sustitución, portabilidad y control efectivo que hoy no está garantizada ni evaluada sistemáticamente.

AC4 DIAGNÓSTICO SECUNDARIO

El régimen federal argentino y la relación con el sector privado y los operadores de servicios esenciales no tienen hoy un canal estable y obligatorio de cooperación en ciberseguridad (la adhesión de provincias a los planes existentes es voluntaria), lo que limita la capacidad nacional de respuesta coordinada ante incidentes que crucen jurisdicciones.

AC5 PRINCIPIO ORIENTADOR PARA LAS RECOMENDACIONES

Es posible construir capacidades soberanas de ciberseguridad sin caer en autarquía tecnológica ni en la promesa de atribución técnica o política irreal, mediante una agenda gradual que distinga lo que el Estado debe controlar directamente, lo que puede compartir bajo condiciones y lo que puede seguir tercerizando con garantías de sustitución y portabilidad.

03 · CONCEPTOS

Conceptos vecinos: ciberdefensa, ciberdiplomacia, ciberinteligencia y protección de datos personales.

La ciberseguridad comparte fronteras con otras cuatro nociones que con frecuencia se confunden entre sí en el debate público: la ciberdefensa, la ciberdiplomacia, la ciberinteligencia y la protección de datos personales. Cada una tiene un fundamento legal propio, un organismo responsable distinto y un objeto de protección diferente. Distinguirlas no es un ejercicio taxonómico: de esa distinción depende saber qué organismo debe actuar frente a cada tipo de incidente, bajo qué control y con qué límites.

NOCIÓN	FUNDAMENTO	ORGANISMO	QUÉ PROTEGE O PRODUCE
Ciberseguridad	Estrategia nacional (Res. 44/2023) y DNU 941/2025	Centro Nacional de Ciberseguridad (CNC)	Activos digitales frente a cualquier amenaza, de origen estatal o no
Ciberdefensa	Ley 23.554 y Decreto 1112/2024	Ministerio de Defensa · Comando Conjunto de Ciberdefensa (CCCD)	Los intereses vitales de la Nación frente a agresiones de origen externo
Ciberinteligencia	Ley 25.520, modificada por el DNU 941/2025	Agencia Federal de Ciberinteligencia (AFC), bajo la SIDE	Inteligencia nacional en y desde el ciberespacio

Ciberdiplomacia	Participación en foros bilaterales y multilaterales	Cancillería, Dirección Nacional de Ciberseguridad y Subsecretaría de Ciberdefensa, sin unidad única	Representación de intereses y normas de conducta responsable
Datos personales	Art. 43 CN, Ley 25.326 y Decreto 1558/2001	Agencia de Acceso a la Información Pública (AAIP)	El derecho individual de las personas sobre su información personal

3.1 Ciberdefensa

La ciberdefensa es la aplicación al ciberespacio de la Ley de Defensa Nacional N° 23.554, que habilita el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar agresiones de origen externo que afecten los intereses vitales de la Nación (art. 2°).

El alcance de qué constituye una "agresión externa" a estos fines fue objeto de una revisión reciente: el Decreto 727/06, que reglamentó esa ley desde 2006, limitaba la agresión habilitante a la proveniente de las fuerzas armadas de un Estado extranjero. El Decreto 1112/2024 (BO 20/12/2024) derogó esa reglamentación sosteniendo en sus considerandos que la propia Ley 23.554 nunca calificó al agresor, sino solo su origen externo, y la reemplazó por una definición más amplia (art. 1°): "se consideran agresiones, el conflicto armado o la guerra que provengan de fuerzas armadas u organismos paraestatales extranjeros, de organizaciones terroristas, de otras organizaciones transnacionales, o de cualquier otra forma de agresión externa incompatible con la Carta de las Naciones Unidas". Se trata de una interpretación del Poder Ejecutivo, no de una reforma de la Ley 23.554 ni de un pronunciamiento judicial, y su constitucionalidad está cuestionada: al menos un proyecto de ley presentado en la Cámara de Diputados en diciembre de 2024 solicita declarar su nulidad, entre otros motivos porque según sus fundamentos habilitaría a las Fuerzas Armadas a cumplir funciones propias de las fuerzas de seguridad.

A diferencia de la ciberseguridad (que protege activos digitales frente a cualquier amenaza, de origen estatal o no) y del ciberdelito (que persigue conductas ilícitas mediante el sistema penal), la ciberdefensa sigue operando únicamente dentro del marco constitucional e institucional de la defensa nacional, con las limitaciones que ese marco impone al empleo de las Fuerzas Armadas en asuntos de seguridad interior; el propio Decreto 1112/2024 (arts. 3° y 6°, inc. b) exige que, en tiempo de paz, esa frontera se administre mediante coordinación entre el Ministerio de Defensa y el Ministerio de Seguridad para la vigilancia y el control de los espacios (incluido el ciberespacial) en que las Fuerzas de Seguridad tengan responsabilidades propias. Se trata de una coordinación acotada a esa función de vigilancia y control, no de un protocolo de notificación de incidentes de ciberseguridad entre organismos, por lo que no contradice el diagnóstico de fragmentación que se desarrolla en el apartado 4, aunque constituye un antecedente institucional relevante si se avanza en esa dirección.

La estructura militar argentina para esta función está compuesta por la Subsecretaría de Ciberdefensa y el Comando Conjunto de Ciberdefensa (CCCD), ambos verificados como órganos activos del Ministerio de Defensa y el Estado Mayor Conjunto; el mismo Decreto 1112/2024 confirmó al CCCD como uno de los comandos conjuntos permanentes del Estado Mayor Conjunto de las Fuerzas Armadas. La Directiva de Política de Defensa Nacional (Decreto 457/2021) fija los lineamientos generales de la defensa para el período, y la Resolución del Ministerio de Defensa 105/2023 actualizó específicamente la "Política de ciberdefensa", creando un Comité de Infraestructuras Críticas de la Información de la Defensa y un centro de supervisión asociado.

El análisis comparado del propio Instrumento Militar Argentino frente a otros países (desarrollado en un estudio especializado dedicado a la ciberdefensa desde una perspectiva de derecho internacional y estrategia militar) describe la doctrina argentina como centrada en el planeamiento estratégico militar y una visión soberana de la defensa, con un grado medio de integración cívico-militar mediante cooperación con la industria nacional y las universidades, y una autonomía operativa media orientada hacia la independencia tecnológica.

La función de "ciberinteligencia" que se despliega dentro de la estructura de ciberdefensa (ámbito militar, orientada a la toma de decisiones del Instrumento Militar) es institucionalmente distinta de la ciberinteligencia que produce el Sistema de Inteligencia Nacional a través de la Agencia Federal de Ciberinteligencia (ámbito civil, bajo la Secretaría de Inteligencia de Estado), que se desarrolla en el apartado 3.2. No se identificó una norma que articule ambas funciones entre sí.

DATO CLAVE — SIN LEY PARA LA CIBERSEGURIDAD CIVIL

No existe en Argentina una "ley" de protección de infraestructuras críticas de información y ciberseguridad. Lo que existe son dos normas de rango infralegal: la Resolución 829/2019 de la entonces Secretaría de Gobierno de Modernización, que aprobó la primera Estrategia Nacional de Ciberseguridad, y la Resolución 1523/2019, que definió los criterios y el glosario de infraestructuras críticas de información. **Ninguna de las dos tiene jerarquía legislativa.**

Este detalle no es menor: la ausencia de una ley en sentido estricto para la ciberseguridad civil (en contraste con la Ley 23.554 que sí sostiene con rango legal a la ciberdefensa militar) es en sí misma un dato relevante para el diagnóstico de fragmentación normativa que este capítulo desarrolla en el apartado 4.

3.2 Ciberinteligencia

La ciberinteligencia, en su acepción institucional argentina vigente, quedó definida por primera vez en una norma de rango legal a partir de la modificación introducida a la Ley de Inteligencia Nacional 25.520 por el mismo decreto que creó el Centro Nacional de Ciberseguridad (DNU 941/2025). Allí se define a la ciberinteligencia como "el desarrollo de las actividades de inteligencia en y desde el ciberespacio", y se asigna su producción a la Agencia Federal de Ciberinteligencia (AFC).

Es indispensable aclarar, porque genera confusión incluso en fuentes especializadas, que la AFC no es la sucesora de la ex-Agencia Federal de Inteligencia (la ex-AFI, actualmente denominada Servicio de Inteligencia Argentino, SIA, sin cambios de nombre por este decreto). La AFC es, en cambio, el resultado de un cambio de nombre de la Agencia Federal de Ciberseguridad, un órgano que hasta la sanción del decreto ya integraba el Sistema de Inteligencia Nacional (SIN). El SIN queda hoy conducido por la Secretaría de Inteligencia de Estado (SIDE) y compuesto por cuatro órganos: el SIA (inteligencia general, sin cambio de nombre), la Agencia Nacional de Contrainteligencia (ANC, ex-Agencia de Seguridad Nacional), la AFC (ex-Agencia Federal de Ciberseguridad, ahora de Ciberinteligencia) y la Inspectoría General de Inteligencia (IGI, ex-División de Asuntos Internos).

La función de la AFC, según la normativa, es "la producción de Inteligencia Nacional sobre actores, hechos, riesgos, oportunidades y amenazas [...] en el ciberespacio y el espacio radioeléctrico". Esta función es jerárquica y funcionalmente independiente del Centro Nacional de Ciberseguridad: mientras la AFC integra el sistema de inteligencia del Estado, bajo la órbita de la Presidencia de la Nación y con el régimen de reserva y control propio de la

actividad de inteligencia, el CNC es un organismo descentralizado de la Jefatura de Gabinete de Ministros con una función civil de ciberseguridad, sin vínculo jerárquico con el sistema de inteligencia. Los propios considerandos del decreto explican esta separación como una decisión deliberada, dirigida a "garantizar la autonomía entre la respuesta a las demandas de ciberinteligencia del [Sistema de Inteligencia Nacional] [...] y las funciones de ciberseguridad que desarrolla la [ex-]AFC".

El control de la actividad de ciberinteligencia recae en el mismo órgano que fiscaliza al resto del sistema de inteligencia: la Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia del Congreso de la Nación, ante la cual la SIDE debe presentar el Informe Anual de Actividades de Inteligencia y a la que deben comunicarse las designaciones del Secretario de Inteligencia de Estado y de los titulares de los organismos del sistema, incluido el de la AFC. No existe, en cambio, un mecanismo de coordinación formal entre esa comisión y los ámbitos de control aplicables al CNC o al CCCD, lo que reproduce a nivel de control parlamentario la misma fragmentación institucional identificada en el **apartado 4** de este capítulo.

Esta arquitectura deja planteada una pregunta que excede el objeto de este capítulo pero que conviene señalar: Argentina tiene hoy, en paralelo y sin coordinación normativa entre sí, al menos dos circuitos institucionales de producción de ciberinteligencia (el de la AFC dentro del sistema de inteligencia civil, y el de "ciberinteligencia y prospectiva" dentro de la estructura militar de ciberdefensa descripta en el **apartado 3.1**), además de la propia función de conocimiento situacional que ejerce el CNC sobre incidentes de ciberseguridad sin ser, en sentido técnico, una agencia de inteligencia. Esta fragmentación funcional refuerza el diagnóstico general de este capítulo sobre la necesidad de articulación entre capacidades existentes, antes que la creación de nuevos organismos.

3.3 Ciberdiplomacia

La ciberdiplomacia es la práctica mediante la cual los Estados representan sus intereses, negocian normas de comportamiento y construyen reglas de conducta responsable para el ciberespacio en foros bilaterales y multilaterales. Su rasgo institucional más visible (documentado en la literatura especializada) es la aparición, desde 2011, de funcionarios diplomáticos dedicados específicamente a esta agenda ("ciberembajadores" o cargos equivalentes), un modelo pionero en Estados Unidos y adoptado luego, con variantes, por Francia, el Reino Unido, Canadá, Australia, Alemania, Estonia e India, entre otros países.

La participación argentina en esta agenda multilateral está documentada, de forma verificable, en varios frentes. Argentina adhirió al Llamado de París para la Confianza y la Seguridad en el Ciberespacio en noviembre de 2018. Participó de los Grupos de Expertos Gubernamentales de Naciones Unidas sobre seguridad de la información en 2013 y 2014, y mantiene participación en el actual Grupo de Trabajo de Composición Abierta (OEWG) de Naciones Unidas sobre esta materia. Es miembro del Foro Global sobre Experiencia Cibernética (Global Forum on Cyber Expertise). Participa, además, activamente del Grupo de Trabajo sobre Medidas de Fomento de la Confianza en el Ciberespacio del Comité Interamericano contra el Terrorismo de la OEA (GT-MFCC/CICTE), según consta en registros de reuniones de 2024. En agosto de 2024, se incorporó formalmente a la Iniciativa Internacional contra el Ransomware (Counter Ransomware Initiative), según el anuncio oficial de la Cancillería argentina. Es, además, parte del Convenio de Budapest sobre Ciberdelito desde 2018 (Ley 27.411), como ya se señaló en el **apartado 1** de este capítulo. Forma también parte del Foro Iberoamericano de Ciberdefensa (FIC), una red de cooperación militar y técnica creada el 27 de mayo de 2016 en Madrid.

Estos antecedentes institucionales tienen una historia previa dentro de la propia administración pública nacional: el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), creado por la Resolución 580/2011 de la entonces Jefatura de Gabinete de Ministros, y el Comité de Ciberseguridad creado por el Decreto 577/2017 (mencionado también en el **apartado 4** de este capítulo como el foro interinstitucional hoy vigente bajo la conducción del CNC) constituyeron los antecedentes organizativos sobre los que se apoyó, en gran medida, la participación internacional de Argentina en esta agenda antes de la creación del CNC.

Este trabajo confirma que Argentina no cuenta con un cargo diplomático formalmente denominado "ciberembajador", a diferencia de los países pioneros mencionados más arriba. La agenda cibernética y digital es atendida, en cambio, de forma distribuida: los registros de participación de Argentina en el Grupo de Trabajo de Composición Abierta de Naciones Unidas muestran intervenciones conjuntas de la Subsecretaría de Política Exterior de la Cancillería, de la Dirección Nacional de Ciberseguridad (organismo técnico, no diplomático) y de la Subsecretaría de Ciberdefensa, sin una unidad única y estable a cargo de la representación internacional en la materia. Este punto (quién representa a la Argentina de forma estable en los foros de ciberdiplomacia) queda señalado como una fragmentación adicional a la ya descripta en el **apartado 4**, y ameritaría una consulta directa a la Cancillería antes de incorporarse como conclusión firme del capítulo.

Cabe señalar, por último, que la ciberdiplomacia no es un campo normativamente homogéneo a nivel global: la literatura especializada documenta modelos de gobernanza divergentes (por ejemplo, el modelo estonio, construido sobre una sociedad digital de base multiactoral, frente a modelos más centralizados en el control estatal del ciberespacio adoptados por otros países), lo que condiciona el tipo de compromisos que Argentina puede razonablemente asumir en cada foro sin comprometer su propio marco institucional interno.

3.4 Protección de datos personales

La protección de datos personales es un régimen jurídico autónomo, de base constitucional (art. 43 de la Constitución Nacional, acción de hábeas data), regulado desde el año 2000 por la Ley 25.326 y su decreto reglamentario 1558/2001. Su autoridad de aplicación es la Agencia de Acceso a la Información Pública (AAIP), organismo descentralizado, que sucedió en estas funciones a la anterior Dirección Nacional de Protección de Datos Personales.

Este régimen protege un objeto distinto del que protege la ciberseguridad institucional descripta en el resto de este capítulo: no se ocupa de la continuidad operativa de sistemas o infraestructuras, sino del derecho individual de las personas sobre su información personal, con independencia de si esa información es vulnerada por un incidente técnico, un uso indebido o una decisión de tratamiento no autorizada. Ambos regímenes se cruzan, sin embargo, en un punto operativo concreto: qué ocurre cuando un incidente de ciberseguridad compromete datos personales.

En ese punto, la Ley 25.326 vigente presenta una limitación verificable: su artículo 9° establece un deber general de adoptar medidas de seguridad para evitar la pérdida o el acceso no autorizado a los datos personales, pero no impone, en el texto legal actualmente en vigor, una obligación expresa de notificar incidentes de seguridad ni a la autoridad de aplicación ni a los titulares de los datos afectados. Una guía de cumplimiento que cita a la AAIP como autoridad de referencia recomienda, como buena práctica derivada del deber general de seguridad del artículo 9°, que el responsable del tratamiento notifique el incidente a la AAIP dentro de las 72 horas de haberlo conocido y que informe también a la persona titular de los datos, en lenguaje claro y sencillo; no se trata, sin embargo, de una obligación legal, sino de una recomendación de buena práctica sin fuerza vinculante propia. Un proyecto legislativo

(Expediente 3661-D-2022) propuso modificar expresamente el artículo 9° para incorporar un “deber de notificación con un plazo de 72 horas”, en línea con estándares internacionales como el Reglamento General de Protección de Datos de la Unión Europea, pero ese proyecto no fue sancionado.

72 h

Plazo de notificación recomendado a la AAIP como buena práctica, sin fuerza vinculante

48 h

Plazo obligatorio de reporte de incidentes para las entidades alcanzadas por la Decisión Administrativa 641/2021

La ausencia de un deber legal expreso de notificación de brechas de datos personales para el sector privado es relevante. La disposición DI-2021-7-APN-DNCIB#JGM instruye que las “entidades y jurisdicciones alcanzadas por la Decisión Administrativa 641/2021 [...] deben reportar los incidentes de seguridad que se produzcan en sus ámbitos, dentro de las CUARENTA Y OCHO (48) horas de tomado conocimiento de su ocurrencia o de su potencial ocurrencia y si hubiera, cuando se produzcan escalamientos significativos”.

Por último, es necesario señalar que la Ley 25.326 atraviesa, al momento de este trabajo, un proceso de reforma con múltiples proyectos en danza, ninguno de los cuales cuenta con dictamen de comisión vigente ni aprobación de ninguna de las cámaras del Congreso. Entre los antecedentes recientes figuran un anteproyecto elaborado por la AAIP en 2022 que obtuvo dictamen pero perdió estado parlamentario en 2024; un proyecto enviado por el Poder Ejecutivo Nacional en 2023 (Mensaje 87/2023); y, ya en el período 2025-2026, al menos cuatro proyectos adicionales presentados por distintos legisladores y por una iniciativa de la sociedad civil (a través de una consulta pública impulsada por organizaciones especializadas), con enfoques que van desde una actualización parcial hasta la derogación completa de la ley vigente y su reemplazo por un régimen de inspiración europea con criterios de proporcionalidad según el tamaño del responsable de tratamiento. Esta pluralidad de proyectos sin definición legislativa es, en sí misma, un dato relevante para el diagnóstico de este capítulo: expresa una demanda de reforma reconocida por distintos sectores políticos, pero también una falta de consenso sobre su contenido que mantiene vigente, por ahora, un régimen sancionado antes de la existencia de buena parte de las tecnologías y los riesgos que hoy plantea el ciberespacio.

04 · DIAGNÓSTICO

El estado institucional argentino: avances recientes y fragmentación persistente.

Argentina dio en el último año y medio un paso institucional de peso: la creación del Centro Nacional de Ciberseguridad (CNC) como organismo descentralizado en la órbita de la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete de Ministros, con el objeto de planificar, ejecutar y supervisar políticas, programas y acciones de ciberseguridad destinadas a proteger el ciberespacio de interés nacional, las infraestructuras críticas de información, los activos digitales estratégicos del Estado Nacional y los sistemas tecnológicos empleados en la prestación de servicios públicos esenciales. El propio decreto le asigna, además,

carácter de órgano rector en materia de protección y seguridad integral del ciberespacio de interés nacional, facultándolo para dictar lineamientos y directivas para todo el Sector Público Nacional, con diecinueve funciones específicas asignadas (DNU 941/2025, art. 24, según cita textualmente la Disposición 1/2026 del propio CNC).

438
Incidentes gestionados por el CERT.ar durante 2024

+15%
Variación respecto del año anterior

19
Funciones específicas asignadas al CNC por el decreto

Bajo esa nueva autoridad, el CERT.ar gestionó 438 incidentes durante 2024, un 15% más que el año anterior, integrando de forma automatizada los reportes de la red regional CSIRT Americas de la Organización de los Estados Americanos, que aportó 265 de esos casos (informe CERT.ar 2024). En mayo de 2026, el CNC dictó además un reglamento de continuidad operativa [5] (cuyo cumplimiento resulta, en sus términos actuales, de extrema dificultad) que exige a todo organismo público un plan de contingencia, un centro de datos alternativo y pruebas anuales de conmutación, con parámetros de tiempo de recuperación definidos según estándares internacionales.

Estas nuevas disposiciones conviven con una fragmentación institucional que la propia normativa reciente no resuelve. El mismo decreto que crea el CNC modificó la Ley de Inteligencia Nacional y renombró a la Agencia Federal de Ciberseguridad como Agencia Federal de Ciberinteligencia (AFC), separando formalmente sus funciones de las del nuevo CNC, sin crear un órgano de coordinación entre ambas (como se dijo en el **apartado 3.2** de este capítulo). El único foro interinstitucional verificablemente activo es el Comité de Ciberseguridad, presidido por el CNC (con base jurídica de 2017 / 2019, que no incluye formalmente a la agencia de inteligencia).

En paralelo, el Ministerio de Seguridad Nacional conserva su propio programa de ciberdelito (el ForCIC [6], creado en enero de 2025) y dictó, dos meses después de la creación del CNC, un "plan federal contra el fraude ciberasistido" [7] que no menciona a la nueva autoridad.

El Banco Central regula, además, la ciberseguridad del sistema financiero por su cuenta, con comunicaciones propias. El resultado es un mapa de competencias donde varias instituciones actúan con variada solvencia en su ámbito, pero sin un protocolo común de notificación cruzada de incidentes ni de deslinde de competencias entre ellas.



Varias instituciones actúan con variada solvencia en su ámbito, pero sin un protocolo común de notificación cruzada de incidentes ni de deslinde de competencias entre el

A esto se suma una incertidumbre normativa no menor: al cierre de este diagnóstico, el decreto que crea el CNC (DNU 941/2025) seguía en trámite ante la Comisión Bicameral Permanente de Trámite Legislativo del Congreso, sin dictamen ni fecha de tratamiento conocida, y con un amparo judicial ya rechazado por falta de legitimación de los demandantes, sin que se analizara el fondo del planteo. El decreto rige mientras tanto por su propia cláusula de vigencia, pero su estabilidad jurídica de mediano plazo no puede darse por comprobada.

Una mirada comparada

Puesto en perspectiva comparada, este patrón no es exclusivo de la Argentina: España mantiene vigente su Estrategia Nacional de Ciberseguridad de 2019 mientras tramita una actualización sin fecha definida; Brasil coordina la ciberseguridad de su administración federal sin una autoridad nacional de alcance general, aunque tiene en el Senado un proyecto para crearla. Chile, en cambio, ya cuenta desde 2025 con una agencia nacional operativa (la ANCI, con potestad de fiscalizar y sancionar tanto a organismos públicos como a privados).

La breve comparación sugiere que la fragmentación argentina no es un fenómeno regional inevitable, sino una etapa de consolidación institucional en la que otros países de la región ya avanzaron con distintos grados de éxito.

05 · ALCANCE

Brechas de alcance: sectores, provincias y municipios.

La capacidad de ciberseguridad del Estado argentino no está distribuida de manera uniforme. En el plano sectorial, el sistema financiero cuenta con un régimen denso de comunicaciones del Banco Central, mientras que no se identificó ninguna norma equivalente para el sector de telecomunicaciones, pese a que esa competencia corresponde formalmente al CNC.

En el plano federal, tres programas nacionales (el ForCIC, el Plan Federal de Prevención de Ciberdelitos 2025-2027 y la DA 641/2021[8]) prevén la adhesión voluntaria de provincias y de la Ciudad de Buenos Aires, pero ninguna de las tres menciona a los municipios como sujetos posibles de adhesión. Esto marca un retroceso respecto de una resolución anterior, ya derogada, que sí los invitaba expresamente a participar.

3 de 3

Programas nacionales que prevén la adhesión voluntaria de provincias y CABA y no mencionan a los municipios

+2.000

Gobiernos locales en el país, de capacidad técnica y presupuestaria muy dispar

Una fuente no oficial (una encuesta de una organización de la sociedad civil sobre un conjunto de municipios argentinos) sugiere que la proporción de gobiernos locales con protocolos de ciberseguridad conocidos o aplicados sería baja; este dato se cita aquí solo como referencia ilustrativa, no como fundamento de las conclusiones de este capítulo, dado que no proviene de una fuente oficial ni de un relevamiento censal.

Esta desigualdad de alcance no debe leerse como ausencia total de capacidad, sino como falta de un canal formal de segundo nivel que permita a los municipios (de capacidad técnica y presupuestaria muy dispar entre sí) sumarse a los esfuerzos nacionales sin que la Nación deba vincularse directamente con cada uno de los más de dos mil gobiernos locales del país.

06 · DEPENDENCIA

La pregunta pendiente: dependencia externa y capacidad de sustitución.

Ningún instrumento normativo argentino evalúa hoy, de manera sistemática y transversal, la dependencia del Estado respecto de proveedores extranjeros de tecnología crítica de ciberseguridad (servicios de nube, sistemas de detección, infraestructura de red) ni su capacidad de sustituirlos en caso de conveniencia estratégica o necesidad. El único antecedente identificado es de 2019, en materia de nube, que formalizó por primera vez con especificaciones técnicas (ONTI) propias de IaaS/PaaS, y que la Disposición 1/2020[9] dejó sin efecto porque excluía a ARSAT.

Es importante señalar que esta brecha no equivale, por sí sola, a una vulnerabilidad demostrada. Este capítulo no asume que toda tecnología extranjera constituya un riesgo por el solo hecho de serlo: la dependencia de proveedores globales es una condición común a la mayoría de los países de la región y del mundo, y sustituirla de forma indiscriminada podría generar más costos que beneficios, como así también soslayar su relevancia estratégica en un mundo susceptible a interferencias o desconexiones tecnológicas. Así también, un diálogo multisectorial reciente de la Corporación Andina de Fomento identificó, en ese sentido, una "ventana de vulnerabilidad" entre la velocidad de adopción tecnológica y la capacidad institucional para gestionarla en América Latina, aunque se trata de una relatoría de encuentro, no de un estudio cuantitativo, por lo que se menciona aquí con esa salvedad.

Lo que la evidencia disponible permite sostener, con mayor solidez, es que el Estado argentino no cuenta hoy con un mecanismo propio para conocer el grado de esa dependencia ni para decidir, con información sistemática, cuándo y cómo diversificar sus proveedores críticos. Esa es la brecha concreta que este capítulo identifica, y es distinta de afirmar que la dependencia actual sea, en sí misma, un riesgo no gestionado.

ANÁLISIS PROSPECTIVO

La fuerte dependencia hacia infraestructuras fuera del territorio nacional (ya sea nube o servicios) conlleva **un riesgo inherente de falta de control soberano, acentuado en escenarios extremos de desconexión global.**

07 · PRINCIPIOS

Principios para construir capacidad sin autarquía.

Del diagnóstico anterior se desprende un criterio rector para cualquier recomendación en esta materia: el problema dominante (no único) de la ciberseguridad argentina es de **articulación entre capacidades ya existentes**, no de ausencia de capacidad. El Centro Nacional de Ciberseguridad, el CERT.ar, el ForCIC, el Banco Central y el sistema universitario y de formación pública ya operan, cada uno en su ámbito, con resultados verificables. La tarea pendiente no es crear una nueva autoridad que los reemplace o los superponga, sino tender los puentes normativos y operativos que hoy faltan entre ellos, y extender su alcance a los sectores, provincias y municipios que quedan hoy fuera de su radio de acción.

Este principio también gobierna la forma en que este capítulo trata la dependencia tecnológica externa: la respuesta que urge no es la localización física obligatoria y probablemente desordenada de datos o proveedores, sino en primera instancia la evaluación sistemática de esa dependencia y el desarrollo de criterios de portabilidad e interoperabilidad que reduzcan el costo de un cambio de proveedor, sin renunciar a los beneficios de la integración tecnológica internacional.

> **La tarea pendiente no es crear una nueva autoridad, sino tender los puentes normativos y operativos que hoy faltan entre las capacidades existentes.**

08 · AGENDA

Recomendaciones.

Sobre esta base, el capítulo propone siete líneas de acción concretas, graduales y verificables, cada una asociada a un responsable institucional ya existente, sin crear organismos nuevos. A ellas se suma una octava recomendación sobre la inclusión de los municipios y el financiamiento.

R1

Protocolo interinstitucional de notificación cruzada

Dictar un protocolo interinstitucional de notificación cruzada de incidentes entre el Centro Nacional de Ciberseguridad, el Ministerio de Seguridad, la Agencia Federal de Ciberinteligencia y el Ministerio de Defensa, con plazos de notificación de entre 24 y 72 horas y un punto de contacto único por organismo. Esta medida no requiere una norma de rango legal y puede implementarse en el corto plazo bajo el paraguas del Comité de Ciberseguridad ya existente; si en doce meses no logra un nivel de cumplimiento verificable, correspondería evaluar dotarla de mayor fuerza vinculante por decreto.

R2

Incorporación municipal graduada

Diseñar un esquema graduado de incorporación municipal a los programas federales de ciberseguridad, canalizado a través de las provincias ya adheridas (no mediante adhesión directa entre la Nación y cada municipio), con niveles de capacidad autoevaluada y un conjunto mínimo de herramientas de continuidad para los gobiernos locales que no cuenten con equipo técnico propio.

R3

Red de SOCs interconectados

Diseñar una red de SOCs (en principio de organismos públicos y gobiernos de segundo y tercer grado) interconectados que permitan un trabajo coordinado que propicie las alertas tempranas.

R4

Evaluación anual de dependencia

Establecer una evaluación anual de dependencia y capacidad de sustitución de proveedores críticos de tecnología de ciberseguridad, a cargo del Centro Nacional de Ciberseguridad con apoyo técnico de la Oficina Nacional de Tecnologías de Información.

R5 **Piloto de intercambio de información entre pares (ISAC)**

Constituir un mecanismo piloto de intercambio de información entre pares (un centro de análisis e intercambio de información, o ISAC, según su denominación internacional) en el sector financiero, por ser el de mayor madurez normativa, con la posibilidad de extenderlo luego a energía, telecomunicaciones y otros sectores si el piloto resulta viable.

R6 **Responsable de Ciberseguridad y carrera pública**

Extender a toda la Administración Pública Nacional el nomenclador de "Responsable de Ciberseguridad" hoy limitado al ámbito de la Sindicatura General de la Nación, como primer paso hacia una carrera pública diferenciada para especialistas en la materia, comenzando por relevar la dotación de personal actualmente disponible, dato que hoy no existe de forma sistemática y pública.

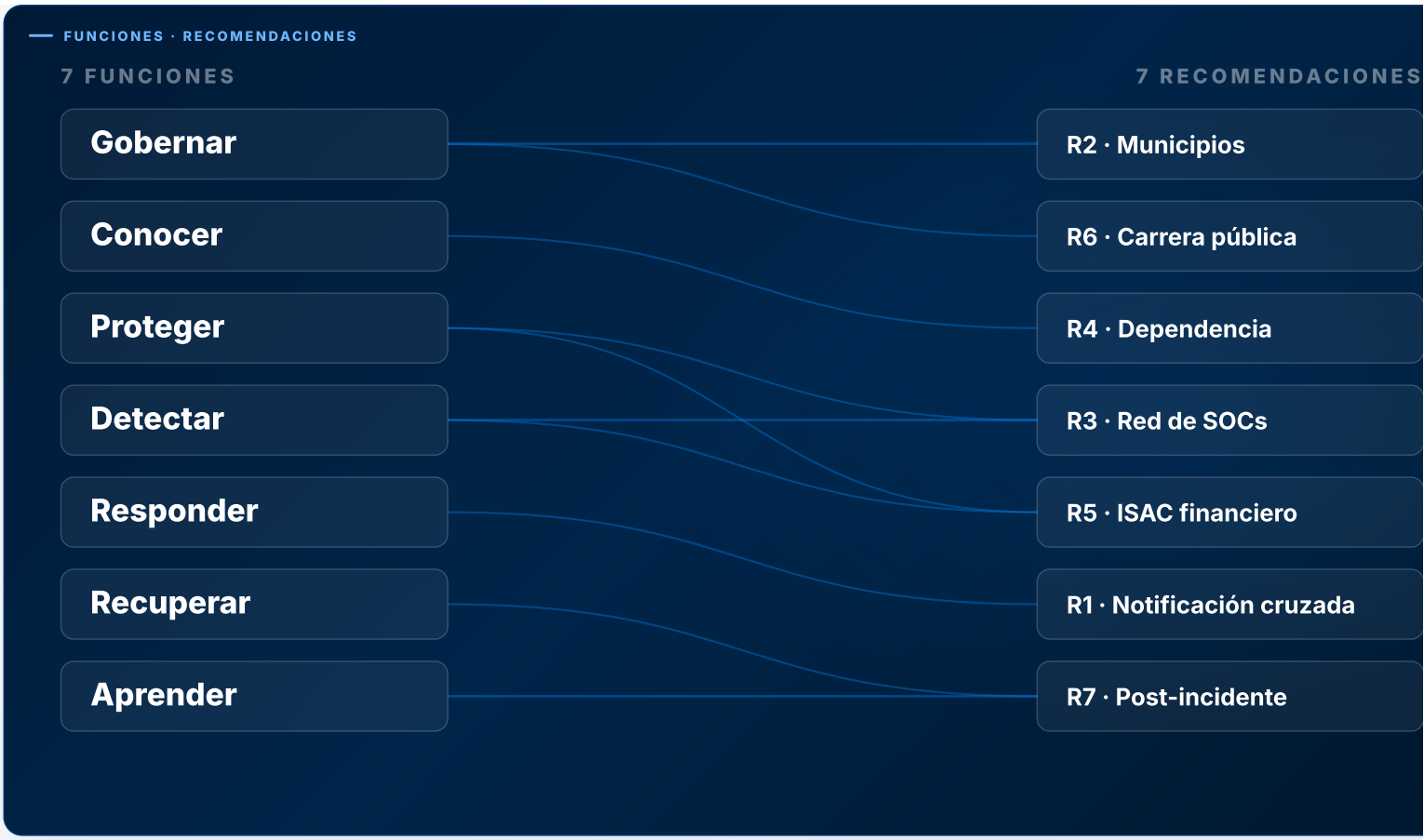
R7 **Informe público post-incidente y simulación conjunta**

Requerir por norma un informe público post-incidente (con las reservas de seguridad que correspondan) para todo incidente que afecte datos personales por encima de un umbral definido o infraestructura crítica, y establecer un ejercicio de simulación conjunta entre organismos, coordinado por el Centro Nacional de Ciberseguridad, distinto de las pruebas internas que cada organismo ya debe realizar por su cuenta.

Cada una de estas líneas se desarrolla, con sus alternativas comparadas, responsables, plazos e indicadores, en el anexo técnico que acompaña a este capítulo.

Qué función fortalece cada recomendación

Leídas en conjunto, estas siete líneas refuerzan puntualmente las funciones descriptas en el apartado 1: la primera fortalece la función de responder, al fijar plazos comunes de notificación entre organismos; la segunda y la sexta, la de gobernar, al extender el alcance institucional a los municipios y profesionalizar la función dentro de la Administración Pública Nacional; la cuarta, la de conocer, al sistematizar información hoy inexistente sobre la dependencia de proveedores críticos; la tercera y la quinta, la de detectar y proteger, mediante la red de SOC y el intercambio de información entre pares; y la séptima, las de recuperar y aprender, mediante el ejercicio de simulación conjunta y el informe público post-incidente.



Siete funciones, siete líneas de acción: qué función refuerza cada recomendación. R8 es transversal y no se asocia a una sola función.

RECOMENDACIÓN ESPECIAL — LA FUNCIÓN DE PROTEGER

La función de proteger requiere además una recomendación especial: si bien ya está cubierta, a nivel normativo en la Administración Pública Nacional, por el reglamento de continuidad operativa del CNC descripto en el apartado 4, **el mismo debe ser reformulado para que deje de ser una norma de cumplimiento inviable.**

R8

Inclusión de los municipios y financiamiento suficiente, sostenido y equitativo

La inclusión de los municipios en el alcance de las normativas de ciberseguridad constituye una condición para construir una política pública verdaderamente federal. Los gobiernos locales forman parte del Estado y tienen responsabilidades sobre información, servicios y derechos de la ciudadanía. Por ello, su participación debe quedar expresamente contemplada, mediante mecanismos de articulación que reconozcan la diversidad de capacidades y realidades territoriales.

La protección de los datos y la continuidad de los servicios públicos requieren una responsabilidad compartida entre los distintos niveles de gobierno. A medida que las administraciones digitalizan sus procesos e intercambian información, la seguridad depende también de las capacidades de cada institución participante. Incluir a los municipios permite construir criterios comunes de prevención, protección y respuesta, e incorporar la perspectiva del nivel de gobierno más cercano a las personas.

Esa inclusión normativa debe acompañarse de políticas públicas con financiamiento suficiente, sostenido y equitativo. Establecer estándares supone prever las condiciones necesarias para cumplirlos: equipos capacitados, infraestructura, asistencia técnica, mantenimiento y actualización permanente. Si esas exigencias recaen exclusivamente sobre los presupuestos locales, se corre el riesgo de profundizar las desigualdades entre municipios y, con ellas, las diferencias en la protección que recibe la ciudadanía.

Por ello, las políticas federales de ciberseguridad deberían contemplar mecanismos de financiamiento y cooperación entre Nación, provincias y municipios, con mayor apoyo a los gobiernos locales que disponen de menos recursos. La asistencia técnica y las capacidades compartidas pueden complementar ese financiamiento y facilitar el cumplimiento progresivo de los estándares.

CIERRE

Una garantía común.

El objetivo debe ser que todos los municipios puedan alcanzar y sostener un nivel adecuado de protección. La seguridad digital de las personas y de los servicios públicos debe constituir **una garantía común**, respaldada por responsabilidades claras y recursos que permitan hacerla efectiva en todo el territorio.

09 · FUENTES

Notas y fuentes.

1. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 ↩
2. https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and ↩
3. https://www.cepal.org/es/publicaciones/81470-construccion-un-ecosistema-confianza-seguridad-digital ↩
4. https://www.argentina.gob.ar/normativa/nacional/resolución-44-2023-389245/texto ↩
5. https://www.boletinoficial.gob.ar/detalleAviso/primera/341893/20260513 ↩
6. https://www.boletinoficial.gob.ar/detalleAviso/primera/319384/20250108 ↩
7. https://www.boletinoficial.gob.ar/detalleAviso/primera/339480/20260316 ↩
8. https://www.argentina.gob.ar/normativa/nacional/decisión_administrativa-641-2021-351345 ↩
9. https://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/342513/norma.htm ↩

SOBRE EL LITAT

Sobre el LITAT.

El **Laboratorio de Innovación y Tecnologías Aplicadas al Trabajo (LITAT)** es una iniciativa de la Asociación Gremial de Computación (AGC) creada para investigar, analizar y generar propuestas sobre el impacto de las tecnologías emergentes —en particular la inteligencia artificial— en el mundo del trabajo.

Su misión es producir conocimiento desde la perspectiva de los trabajadores, garantizando que la incorporación tecnológica no vulnere derechos laborales ni profundice desigualdades. Tiene su Dirección y se organiza a través de un Consejo Asesor integrado por especialistas técnicos, investigadores y referentes temáticos, y cuenta con áreas de trabajo dedicadas a temas como la transformación de roles ocupacionales, la economía de plataformas, la protección de datos, la soberanía tecnológica, la ciberseguridad y la formación profesional.

Guiado por los principios de **ética, transparencia, soberanía tecnológica y colaboración**, el LITAT actúa como referente sindical en el debate sobre el futuro del trabajo en la era digital, con alianzas estratégicas con universidades, sindicatos, organismos públicos y organizaciones de la sociedad civil a nivel nacional e internacional.

Leer el documento "Soberanía digital en Argentina" →

LITAT

Una iniciativa de la **Asociación Gremial de Computación**