

Perspectivas estratégicas

para el Desarrollo Humano
Integral de la Argentina

Prólogo de Itai Hagman

Gonzalo Armua
Ulises Bosia
María Gimena Cánepa
Romina Chuffardi
Bruno Giormenti Moravec
Comps.

PARA UNA NUEVA INTELIGENCIA NACIONAL: NORMATIVA, DIAGNÓSTICO Y LINEAMIENTOS PROPOSITIVOS

Equipo de Inteligencia de la Fundación DHI



Equipo de Inteligencia de la Fundación DHI

Se dedica al estudio y análisis de las políticas vinculadas al sistema de inteligencia nacional, con especial atención a su marco normativo, su arquitectura institucional y sus prácticas de conducción y control. Busca establecer lineamientos para una futura política que conjugue eficacia y responsabilidad democrática, para el desarrollo de una inteligencia orientada al pueblo y a los intereses estratégicos de la Nación, que opere dentro de límites claros con mecanismos de supervisión y transparencia.

INTRODUCCIÓN

Durante décadas, el debate público sobre los servicios de inteligencia quedó capturado por una alternativa falsa: o se los concebía como instrumentos necesarios del poder —con toda la opacidad y discrecionalidad que esa concepción habilita— o se los reducía a un problema de vulneración de derechos por parte del Estado que era preciso limitar, vigilar y, en lo posible, neutralizar. Esa tensión irresuelta explica, en buena medida, por qué ninguna de las reformas que se sucedieron desde la recuperación democrática logró construir un sistema legítimo y funcionalmente eficaz al mismo tiempo.

Este documento parte de una premisa diferente: la inteligencia nacional, entendida en sentido propio, es una función de conocimiento estratégico del Estado. Es la capacidad que tiene un Estado para reducir la incertidumbre que rodea sus decisiones más importantes: qué ocurre en su entorno, qué actores lo condicionan, qué riesgos se aproximan antes de que se vuelvan crisis, qué oportunidades existen para fortalecer su posición soberana. Producto de la carencia de una cultura de inteligencia, se la ha concebido como un instrumento de vigilancia política y un apéndice del poder de turno. Un Estado que carece de esa capacidad no decide con autonomía, sino que se limita a reaccionar y/o delegar en otros —con frecuencia en actores externos— la tarea de interpretar el entorno por él.

Bajo esta concepción, la inteligencia no se agota en la seguridad en sentido estricto. Abarca también la protección de los recursos estratégicos y las capacidades científico-técnicas nacionales, la evaluación de escenarios internacionales que inciden en el desarrollo del país, la detección temprana de interferencias sobre el proceso decisorio del Estado y la preservación de la autonomía política, tecnológica y económica de la Nación. Producir inteligencia soberana es, en este sentido, una condición del ejercicio efectivo del gobierno.

Para un proyecto nacional y popular, esta dimensión tiene una relevancia de orden estratégico que no admite ser postergada. Un gobierno que se propone transformar las condiciones de vida de su pueblo, recuperar márgenes de

soberanía económica y proyectar al país en el escenario internacional enfrenta resistencias multidimensionales.

Si el Estado no comprende y analiza la relevancia de fenómenos tales como los recursos naturales, la presión de los mercados financieros, las operaciones de desestabilización, la captura de organismos del Estado o la dependencia tecnológica ingresa en una posición de desventaja estructural, sin márgenes de decisión para un desarrollo armonioso del bien común.

El documento que sigue se organiza en cuatro partes. La primera reconstruye el derrotero normativo e institucional del sistema desde la Ley N° 25.520 de 2001 hasta el DNU N° 941/2025, identificando los patrones de continuidad y ruptura que atraviesan las sucesivas reformas. La segunda ofrece un diagnóstico de las causas estructurales que explican por qué ninguna de esas reformas logró consolidarse. La tercera presenta los objetivos generales y las propuestas concretas de reorganización del Sistema de Inteligencia Nacional, incluyendo sus subsistemas especializados, el diseño del control externo e interno y los lineamientos para la profesionalización del personal. La cuarta desarrolla los fundamentos doctrinarios que deben orientar la actividad. El hilo conductor de todas las secciones es el mismo: la inteligencia solo puede cumplir su función estratégica si opera con legitimidad social, dentro de un marco institucional estable y con una doctrina construida desde los intereses nacionales.

1. SECCIÓN NORMATIVA

Búsquedas y derivas del Sistema de Inteligencia Nacional

El sistema de inteligencia argentino atravesó en los últimos veinticinco años un proceso de reformulación normativa e institucional que expresa intentos sucesivos del Estado por dotar a esta actividad de un marco democrático controlado y funcionalmente eficiente. La Ley N° 25.520 de 2001 estableció la arquitectura institucional respetando la separación entre la seguridad interior y la defensa nacional, y fijó principios de legalidad, proporcionalidad y control civil.

La norma definió la producción de inteligencia nacional como una función del Estado dirigida a identificar hechos, riesgos y conflictos que afecten la seguridad interior o la defensa nacional, así como las oportunidades para la consecución de los intereses estratégicos de la Nación, y prohibió expresamente toda actividad de carácter represivo o policial. El Sistema de Inteligencia Nacional (SIN) se estructuró bajo la conducción de la Secretaría de Inteligencia, dependiente de la Presidencia, en coordinación con los organismos de inteligencia de la Defensa y de Seguridad.

Como mecanismo de fiscalización parlamentaria se creó la Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia (CBI), con competencia sobre el uso de fondos reservados y la legalidad de las actividades de los servicios; aunque su funcionamiento efectivo resultó, en la práctica, sistemáticamente débil bajo todas las administraciones que se sucedieron.

En 2015, la convergencia de una crisis de conducción interna en la Secretaría de Inteligencia —expresada en el desplazamiento del director de Operaciones Antonio Stiuso en diciembre de 2014— con el impacto institucional de la muerte del fiscal Alberto Nisman en enero de ese año, desencadenó una reforma que derivó en la Ley N° 27126. Esta normativa sustituyó la Secretaría de Inteligencia por la Agencia Federal de Inteligencia (AFI), estableció una conducción integrada por un Director General y un Subdirector General designados con acuerdo del Senado, e incorporó al objeto de la ley la producción de inteligencia criminal sobre delitos federales complejos. Su innovación más relevante desde el punto de vista de la responsabilidad individual fue el artículo 5° bis, que prohibió expresamente la obediencia debida como eximente y exigió que toda actividad de inteligencia fuera ordenada por las máximas autoridades del organismo.

El Decreto N° 1311/2015, de julio de aquel año, aprobó una nueva doctrina de inteligencia nacional concebida como un cuerpo doctrinario destinado a orientar un proceso de reforma y modernización del SIN. Según el texto del decreto, esta doctrina parte de una visión integral de la inteligencia, entendida como una actividad institucional del Estado que se desarrolla dentro del marco del Estado constitucional y que busca dar cuenta de los desafíos, coacciones y conflictos que ponen en riesgo la defensa y la seguridad democrática. La norma reafirmaba la subordinación civil, la transparencia administrativa y la integración de capacidades técnicas.

Sin embargo, el cambio de administración en diciembre de 2015 derivó en la derogación de gran parte de esta reglamentación: reinstauró la opacidad de la organización y amplió la intervención de la AFI en investigaciones judiciales, lo que provocó una superposición de funciones con las fuerzas de seguridad federales y un retroceso en términos de control institucional.

En 2019, mediante el Decreto N° 52, el Poder Ejecutivo dispuso la intervención de la AFI, con el objetivo de revertir un proceso de regresión institucional iniciado con el Decreto N° 656/2016, que había restablecido el carácter secreto de la estructura orgánica, del régimen de personal y del manejo de fondos del organismo, lo que en aquel entonces implicó un retroceso respecto de los principios de transparencia, publicidad y control civil establecidos por la Ley N° 27126 y por el Decreto N° 1311/2015, afectando el cumplimiento de los fines legítimos

de la inteligencia estatal en el marco de un Estado de derecho. La intervención fue concebida como una medida destinada a restablecer la vigencia del orden normativo anterior, reorganizar el sistema, revisar las estructuras y prácticas internas de la AFI y garantizar la adecuación de la actividad de inteligencia a los principios democráticos, republicanos y de respeto por los derechos y garantías constitucionales. Este intento de reordenamiento del SIN trajo como consecuencia la pérdida de capacidades en la actividad de inteligencia y la inauguración de un ciclo ininterrumpido de intervenciones.

En 2024, los Decretos N° 614 y 615 plantearon una nueva organización del sistema. Se dispuso la disolución de la AFI y la restitución de la Secretaría de Inteligencia del Estado (SIDE). La nueva estructura incorporó cuatro componentes: el Servicio de Inteligencia Argentino (inteligencia exterior), la Agencia de Seguridad Nacional (inteligencia interna), la Agencia Federal de Ciberseguridad (protección de infraestructuras críticas) y la División de Asuntos Internos (control interno).

El Decreto N° 941/2025, firmado el 31 de diciembre de 2025 y publicado como DNU sin acreditar urgencia excepcional, modificó la Ley N° 25.520 en varias direcciones convergentes. Declaró encubiertas por defecto todas las actividades de inteligencia nacional; extendió las obligaciones de contrainteligencia —incluyendo las medidas de seguridad pasivas— a todo el Sector Público Nacional bajo responsabilidad de cada titular de organismo; y habilitó al personal de inteligencia a aprehender personas en casos de flagrancia o requerimiento judicial, atribución históricamente reservada a las fuerzas policiales. El decreto también introdujo dos nuevas estructuras de coordinación: la Comunidad de Inteligencia Nacional (CITN), que integra bajo dirección de la SIDE a los organismos del SIN, las áreas de inteligencia de las fuerzas armadas, policiales y de seguridad federales, y otros organismos del sector público con competencias afines; y la Comunidad Informativa Nacional (CIFN), que incorpora bajo la misma dirección a organismos públicos con capacidad de generar insumos informativos de interés para el sistema. Finalmente, disolvió la Dirección Nacional de Inteligencia Estratégica Militar —único organismo de inteligencia militar con dependencia directa del Ministro de Defensa— transfiriendo sus funciones, bienes y personal a la Dirección General de Inteligencia del Estado Mayor Conjunto. Esta reconfiguración desdibuja la separación entre inteligencia estratégica, defensa nacional y seguridad interior, y concentra en la SIDE una capacidad de dirección sobre el conjunto del aparato estatal que no tiene precedente en el período democrático.

2. DIAGNÓSTICO

Captura política, carencia de efectividad y sumisión geopolítica

La inteligencia argentina enfrenta una crisis estructural, cuyas causas se mantienen con matices. Marcelo Sain (2016) las caracteriza como “patologías institucionales de origen político”: los servicios de inteligencia se desarrollaron históricamente como instrumentos del poder faccioso antes que como una función del Estado, y esa lógica fundacional nunca fue revertida por las reformas que se sucedieron en el período democrático. De allí se desprenden problemas que se refuerzan mutuamente y que ningún rediseño normativo logró resolver de fondo.

El primero es la captura política del sistema. La dependencia directa del presidente, la ausencia de contrapesos institucionales reales y el uso reiterado de los servicios para fines ajenos a sus funciones —vigilancia y persecución política, presión judicial, injerencia interna— erosionaron tanto la legitimidad pública como la profesionalización de los agentes. Esta lógica consolidó una cultura organizacional basada en los compromisos personales y la obediencia política antes que en la competencia técnica. Como señala Iván Poczynok (2023), los escándalos acumulados a lo largo de las décadas democráticas forjaron una agenda reformista orientada casi exclusivamente a reducir la autonomía y el secretismo de los servicios, postergando de manera sistemática la pregunta sobre su efectividad. El déficit de legitimidad se agravó por la opacidad en el manejo de fondos reservados y la escasa rendición de cuentas ante los organismos de control. Si bien la Comisión Bicameral de Fiscalización existe formalmente, su capacidad operativa fue limitada por la ausencia de recursos técnicos, personal especializado y criterios homogéneos. El control efectivo se ejerció de modo reactivo y políticamente condicionado, antes que como auditoría técnica permanente.

El segundo problema es la pérdida acumulada de capacidades operativas. Los ciclos recurrentes de purga y reemplazo de personal desarticulaban el cúmulo de conocimiento técnico y quebraron la transmisión de experiencia. En lugar de consolidar un sistema basado en la obtención y el análisis sistemático de información estratégica, la actividad se configuró de manera fragmentaria, condicionada por coyunturas políticas. Retomando a Sain (2016), las prácticas institucionales demostraron capacidad de adaptación sin transformación: las reformas alteran estructuras y denominaciones, pero no modifican las rutinas internas ni la cultura organizacional, que se reproduce a través de redes informales de lealtad personal. Una consecuencia concreta de este proceso es que algunas fuerzas de seguridad cuentan con mejores herramientas tecnológicas que el propio sistema

de inteligencia nacional, mientras el ciclo de producción —desde la planificación hasta la difusión— quedó estanco.

El tercer problema, que atraviesa a los anteriores, es la ausencia de una doctrina propia y de una definición autónoma de amenazas. La inestabilidad institucional y la falta de conducción política sostenida impidieron el desarrollo de una estrategia nacional de inteligencia. Cada administración impuso su propia orientación, modificando estructuras y prioridades, derivando en un sistema discontinuo donde las tensiones entre ministerios, la competencia por recursos y la falta de interoperabilidad tecnológica generaron duplicación de tareas y pérdida de capacidad estratégica. Sin una definición clara de qué constituye una amenaza para la Nación, la actividad quedó sujeta a criterios coyunturales antes que a políticas de largo plazo.

Pero esa indefinición tiene también una dimensión externa que el debate local tiende a soslayar. En materia de terrorismo y narcotráfico (o “narcoterrorismo”), los marcos conceptuales, las hipótesis de amenaza y buena parte de la tecnología operativa fueron históricamente provistos o fuertemente condicionados por actores externos. La adopción acrítica de esas agendas no fue neutral: orientó las prioridades del sistema hacia problemas definidos desde afuera, con criterios que no siempre coincidieron con los intereses estratégicos nacionales y que introdujeron dinámicas de dependencia operativa difíciles de revertir. Según José María Damsky (2018), las dificultades del país para desplegar un proyecto nacional con plena independencia se deben en parte a que los habitantes y el Estado carecen de una visión estratégica para ejercer sobre el propio territorio vital un control soberano pleno. Como resultado el sistema de inteligencia representa uno de los síntomas más claros, porque es precisamente en este ámbito donde la autonomía estratégica se juega de manera más silenciosa y decisiva.

El diagnóstico que arroja este análisis es que no hubo reforma estatal capaz de articular legitimidad con efectividad ni construir una doctrina nacional estable para el SIN. Las modificaciones normativas que se sucedieron desde 2001 respondieron más a crisis políticas que a diagnósticos técnicos, y sus efectos fueron sistemáticamente interrumpidos antes de consolidarse.

3. OBJETIVOS GENERALES

La pregunta que organiza estos objetivos es qué tendría que ser diferente para que una reforma del sistema de inteligencia argentino no termine como las anteriores. El diagnóstico acumulado en más de dos décadas de ciclos reformistas fallidos ofrece una respuesta incómoda: las causas del problema se refuerzan

mutuamente y ninguna intervención que las aborde por separado lograría revertirlas. Un sistema capturado difícilmente construye doctrina propia, y sin doctrina propia tampoco puede definir con criterios soberanos qué capacidades tecnológicas necesita desarrollar, ni de quién puede depender para hacerlo.

Esta propuesta parte de esa interdependencia y la toma como principio organizador:

- **Legitimidad y cultura estratégica.** Construir una base de consenso social sobre el rol estratégico de la inteligencia como función del Estado, disociándola de su historia de uso político discrecional. Sin legitimidad social, ninguna reforma técnica o normativa es sostenible.
- **Autonomía doctrinaria y definición soberana de amenazas.** Desarrollar una doctrina nacional de inteligencia que defina con criterios propios las amenazas estratégicas, superando la dependencia conceptual y tecnológica respecto de actores externos. La inteligencia debe ser parte del núcleo de un proyecto de Estado, no un apéndice de agendas foráneas.
- **Reorganización funcional del sistema.** Estructurar el Sistema de Inteligencia Nacional bajo la conducción de la SIDE en la Jefatura de Gabinete, integrando los subsistemas especializados —criminal, defensa, científico-técnico e integrado— con marcos analíticos compartidos y criterios comunes de producción.
- **Soberanía tecnológica.** Desarrollar capacidades propias de obtención, análisis y gestión de información, incluyendo infraestructura digital soberana que elimine la dependencia de proveedores externos en el manejo del conocimiento estratégico nacional.

4. PROPUESTAS

Caracterización de las actividades de inteligencia

El sistema de inteligencia argentino no tiene legitimidad social porque fue mayormente utilizado sin principios ni objetivos nacionales. Pero también porque nunca se explicó con claridad para qué sirve cuando funciona bien. Antes de reorganizar estructuras o rediseñar subsistemas, es necesario construir una base de consenso social sobre el rol estratégico de la inteligencia en una comunidad. Consideramos que el punto transversal a cualquier política de planificación de inteligencia debe ser en primera instancia la legitimación social de este campo: la construcción de una cultura de inteligencia. Ese es el punto de partida de estas propuestas.

La seguridad nacional, entendida en su dimensión estratégica, abarca la protección de la soberanía política y territorial, la integridad de la infraestructura crítica y los recursos estratégicos, sin disolver la distinción entre defensa nacional y seguridad interior, que constituye un principio estructurante del sistema normativo argentino. Esa distinción no limita la concepción de seguridad, sino que define los instrumentos legítimos con que cada componente del sistema puede operar. Bajo esta concepción, la inteligencia debe ser un instrumento para la toma de decisiones estratégicas del Estado: su función no es intervenir en la política interna, sino reducir la incertidumbre que rodea las decisiones de quienes la conducen.

La SIDE funcionará en el ámbito de la Jefatura de Gabinete de Ministros, dejando de responder directamente a la Presidencia. Esta decisión no es menor, ya que anclar la conducción de la inteligencia en el órgano constitucionalmente responsable de la coordinación interministerial es una forma de institucionalizar su función para evitar su subordinación discrecional. La SIDE es el órgano rector del Sistema de Inteligencia Nacional, responsable de la dirección, coordinación y supervisión de todos los subsistemas. Su misión consiste en definir las políticas generales de inteligencia, establecer lineamientos estratégicos, consolidar la planificación nacional y garantizar la coherencia doctrinaria del sistema.

Las actividades de inteligencia que llevará a cabo la SIDE serán fundamentalmente tres:

La producción de inteligencia estratégica es el proceso continuo por el cual la SIDE obtiene, procesa y analiza información para convertirla en conocimiento útil para la toma de decisiones de alto nivel. La inteligencia nacional debe captar señales del entorno, anticipar escenarios y traducir esa comprensión en opciones concretas para quienes deciden. La inteligencia reduce la incertidumbre que rodea las decisiones estratégicas. Un Estado con inteligencia soberana decide con autonomía y preserva una tarea que le es constitutiva.

La contrainteligencia debe entenderse en un sentido más amplio que la mera detección de riesgos y amenazas extranjeros. Su propósito es proteger la autonomía política, tecnológica y económica de la Nación frente a injerencias o presiones tanto externas como internas. Esto incluye resguardar la integridad del proceso decisorio estatal: que las decisiones del Estado sean efectivamente del Estado nacional.

La ciberinteligencia es la capacidad de producir conocimiento sobre actores, intenciones y capacidades que operan en el ciberespacio con potencial de afectar los intereses nacionales. A diferencia de la ciberdefensa —que protege y opera infraestructura crítica— y de la persecución del cibercrimen —que corresponde al ámbito de la seguridad interior—, la ciberinteligencia tiene como función

identificar quién actúa, con qué objetivos y con qué medios en el dominio digital, y convertir ese conocimiento en insumo para la toma de decisiones estratégicas del Estado. En ese sentido, la ciberinteligencia pertenece al núcleo de funciones que la SIDE conduce como órgano rector del sistema. La SIDE podrá formular requerimientos y solicitar apoyo técnico operativo a los organismos de defensa con capacidad instalada en este dominio, pero la producción del conocimiento estratégico sobre el ambiente cibernético es una función que no puede delegarse sin perder coherencia doctrinaria. Argentina enfrenta aquí un problema estructural que el Decreto N° 941/2025 no resolvió: la multiplicidad de organismos con jurisdicción sobre el dominio digital —incluyendo la Agencia Federal de Ciberinteligencia creada por el propio decreto— sin una arquitectura clara que defina jerarquías, evite superposiciones y acumule capacidades en lugar de dispersarlas.¹

Clasificaciones de seguridad de la información

Estas funciones comparten una condición que las distingue de cualquier otra actividad estatal: el secreto. En una democracia, la transparencia es la regla general del funcionamiento del Estado. La inteligencia es una excepción legítima a esa regla, pero el secreto debe estar acotado por la ley, supervisado por organismos de control y orientado exclusivamente a la protección del interés nacional. Cuando el secreto protege intereses particulares o persigue adversarios políticos deja de ser una herramienta del Estado.

Frente a este escenario, resulta imperativo recuperar un sistema de clasificaciones graduadas que permita ordenar el flujo de información dentro de un sistema de inteligencia que opera en colaboración con múltiples organismos estatales. La experiencia comparada ofrece un marco de referencia útil: el modelo español articulado por la Oficina Nacional de Seguridad del Centro Nacional de Inteligencia (CNI), que establece cuatro niveles de clasificación —Secreto, Reservado, Confidencial y Difusión Limitada— organizados según el daño potencial que la divulgación no autorizada causaría a los intereses del Estado. Lo

1. El Comando Conjunto de Ciberdefensa (CCCD), creado en 2014 bajo el Estado Mayor Conjunto de las Fuerzas Armadas, constituye la principal capacidad operativa argentina en este dominio y cuenta con antecedentes concretos en protección de infraestructura crítica nacional. Su situación actual es preocupante: la venta de su sede operativa en Puerto Madero y el fracaso de las licitaciones para renovar equipamiento lo dejaron desfinanciado y sin sede definitiva, a contramano de la tendencia regional. A modo de ejemplo, Colombia se consolidó como referencia en América Latina, ya que construyó una arquitectura de carriles diferenciados —coordinación desde el Ministerio TIC, operaciones militares desde el Comando Conjunto Cibernético y persecución del cibercrimen desde la Policía— que produjo resultados concretos: una reducción del 48% en los incidentes cibernéticos durante 2025, que pasaron de 1.427 casos gestionados en 2024 a 697 en 2025.

relevante de ese esquema no es solo su gradación descendente de sensibilidad, sino la función que cumple el nivel inferior: la categoría de Difusión Limitada no implica apertura pública, sino circulación interna restringida entre organismos estatales habilitados, sin exigir habilitación personal de seguridad individual. Es, en otros términos, el escalón que permite la colaboración interagencial.

Adaptado al contexto argentino y a la arquitectura de una Comunidad de Inteligencia Nacional que incorpora organismos de distinta naturaleza institucional, ese esquema podría replicarse con las siguientes categorías:

Secreto, reservado a información cuya divulgación comprometería gravemente la seguridad del Estado, clasificable únicamente por el órgano rector del sistema.

Reservado, para información sensible de acceso restringido a organismos de inteligencia y fuerzas de seguridad con habilitación específica.

Confidencial, accesible a organismos estatales colaboradores bajo habilitación ministerial.

De Circulación Restringida, categoría destinada a reemplazar la noción de “público” en contextos internos, que permite el intercambio entre organismos autorizados dentro del sistema sin que esa información quede sujeta al régimen de encubrimiento ni sea considerada de acceso irrestricto. Esta última categoría es la que resuelve la tensión estructural que el Decreto N° 941/2025 generó al declarar encubiertas todas las actividades de inteligencia por defecto: bajo ese esquema, un organismo colaborador que produce o recibe información en el marco del sistema no sabe qué puede compartir ni con quién, lo que genera una sobreclasificación por precaución que es disfuncional para el propio sistema que se pretende fortalecer.

La incorporación de un nivel de difusión pública activa responde a una concepción precisa del rol que debe cumplir el sistema de inteligencia en una democracia: la defensa del orden constitucional como mandato unívoco. El modelo alemán del Bundesamt für Verfassungsschutz (BfV) ilustra esta idea con claridad a través de la publicación anual del Verfassungsschutzbericht, un informe orientado a formar a la ciudadanía en la comprensión de las amenazas que enfrenta el sistema democrático. Para el sistema argentino, asumir este mandato implicaría que la SIDE comunique activamente las amenazas al orden constitucional, los marcos que la contienen y los límites que la regulan.

La experiencia brasileña aporta un elemento comparativo útil. Tras la crisis de legitimidad de la Agencia Brasileña de Inteligencia (ABIN) durante el gobierno de Jair Bolsonaro —donde recursos de inteligencia del Estado fueron usados para espiar a periodistas, jueces y opositores—, Brasil canalizó la función de defensa democrática hacia un organismo jurídico externo al sistema de inteligencia, inspirado conceptualmente en el modelo alemán. La decisión fue comprensible en

contexto, pero fragmentó esa función en lugar de fortalecerla desde adentro. La propuesta que aquí se sostiene toma el camino inverso: hacer de ese mandato el núcleo que le otorga sentido a la SIDE —hacia adentro como identidad que cohesiona a sus agentes, hacia afuera como base para una cultura de inteligencia sostenible en el tiempo.

Subsistemas del Sistema Nacional de Inteligencia

En la búsqueda de construir un sistema de inteligencia legítimo y efectivo se requiere una estrategia integral basada en tres ejes: conducción política, profesionalización técnica y delimitación funcional clara. Para eso cada subsistema debe cumplir funciones específicas bajo una fuerte conducción política y dentro de un marco común de planeamiento.

Bajo su conducción u orientación deben integrarse de manera efectiva los subsistemas específicos:

- Subsistema de Inteligencia Criminal (SICRI), dependiente del Ministerio de Seguridad, orientado a la producción de inteligencia criminal sobre delitos federales complejos y fenómenos delictivos organizados que afecten la seguridad interior.
- Subsistema de Inteligencia de la Defensa (SIDEF), bajo el Ministerio de Defensa, responsable de la inteligencia estratégica militar vinculada a la defensa nacional y a las amenazas estatales y de actores externos.
- Subsistema de Inteligencia Científico-Técnica (SITEC), con participación de organismos especializados en tecnologías de la información, protección de infraestructuras críticas y del ciberespacio.
- Subsistema Argentino de Inteligencia Integrada (SAII), integración de organismos de la Administración Pública que directa o indirectamente produzcan conocimientos de interés para las actividades de inteligencia.

Cada subsistema debe articular su planeamiento a partir de las directrices emitidas por la SIDE, asegurando la interoperabilidad técnica, la trazabilidad de la información y la uniformidad doctrinaria en la producción de inteligencia.

Para cumplir con estas misiones se deberá crear un Consejo de Inteligencia Nacional que unifique criterios, defina los riesgos y las amenazas prioritarias y articule las capacidades de los distintos organismos bajo un plan estratégico común. Ese plan estará integrado por representantes de cada área que, además de tener claros los lineamientos, deberán garantizar la funcionalidad del sistema para evitar también la superposición entre áreas.

Subsistema de Inteligencia Criminal (SICRI)

Las redes delictivas de escala que engloban el narcotráfico, la trata de personas, el lavado de activos y las economías ilegales territorializadas operan con estructuras complejas, vínculos transnacionales y capacidad de penetración institucional. Combatirlas con herramientas diseñadas para la prevención del delito común es una respuesta estructuralmente inadecuada. La inteligencia criminal no reemplaza a las fuerzas de seguridad, sino que produce el conocimiento estratégico que ninguna fuerza puede producir por sí sola.

El SICRI funcionará bajo la conducción técnica del Ministerio de Seguridad. Su órgano rector es la Dirección Nacional de Inteligencia Criminal (DNIC), cuya función no se agota en la producción de inteligencia propia, sino que avanza en la articulación e integración del conjunto del subsistema. La DNIC conduce el SICRI sin reemplazar a los organismos que lo integran: fija los lineamientos analíticos, establece los estándares de producción y garantiza que la información fluya de manera coherente hacia la SIDE y hacia los usuarios operativos del sistema.

El SICRI integra bajo la conducción de la DNIC a las unidades de inteligencia criminal de las fuerzas federales —Policía Federal Argentina, Gendarmería Nacional, Prefectura Naval Argentina y Policía de Seguridad Aeroportuaria— y a las policías provinciales mediante convenios de adhesión. Cada fuerza mantiene su estructura de inteligencia criminal propia; lo que el subsistema aporta es el marco común que permite que esa información se acumule, se cruce y se analice de manera integrada en lugar de permanecer fragmentada en silos institucionales.

Su misión es producir conocimiento estratégico sobre redes delictivas, economías ilegales, corrupción institucional y amenazas híbridas, siempre con un horizonte de anticipación. Para que esa articulación sea efectiva, el SICRI adoptará criterios comunes de obtención, análisis, diseminación y resguardo de información, garantizando interoperabilidad técnica y estandarización de los productos. La fragmentación de bases de datos y la incompatibilidad de sistemas entre jurisdicciones han sido históricamente los principales obstáculos operativos del sistema.

Subsistema de Inteligencia de la Defensa (SIDEF)

El SIDEF funcionará bajo el Ministerio de Defensa y su misión es producir inteligencia estratégica militar orientada a la protección de la soberanía, la defensa territorial y la anticipación de amenazas externas. Eso incluye el monitoreo de capacidades militares regionales, la evaluación de escenarios de conflicto y el análisis de actores estatales y no estatales de origen externo que representen amenazas a la soberanía o la integridad territorial argentina. También corresponde recuperar

la contrainteligencia militar, área históricamente desatendida que adolece además de un marco normativo claro.

El órgano rector del SIDEF es la Dirección Nacional de Inteligencia Estratégica Militar (DNIEM), cuya restitución es una condición para que el subsistema opere con conducción civil efectiva. La disolución de la DNIEM por el Decreto N.º 941/2025 —que transfirió sus funciones a la Dirección General de Inteligencia del Estado Mayor Conjunto— concentró toda la inteligencia militar bajo conducción castrense, sin contrapeso civil directo. La DNIEM restituida dependerá directamente del Ministro de Defensa y tendrá como función conducir e integrar al conjunto del subsistema, fijar los lineamientos analíticos en coordinación con la SIDE y garantizar que la producción de inteligencia militar responda a prioridades definidas políticamente.

Bajo la conducción de la DNIEM, el SIDEF integra a las direcciones de inteligencia de las tres fuerzas armadas —Ejército, Armada y Fuerza Aérea— cada una de las cuales mantiene su estructura propia orientada a sus necesidades específicas. La función integradora de la DNIEM no suprime esas estructuras, sino que las articula bajo un marco analítico común y garantiza que su producción sea coherente con las prioridades del sistema nacional.

Subsistema de Inteligencia Científico-Técnica (SITEC)

El SITEC producirá conocimiento estratégico sobre el Estado y la evolución de las capacidades tecnológicas propias y ajenas, y orientará las decisiones del Estado en materia de desarrollo soberano. A diferencia de los demás subsistemas, el SITEC no cuenta con un organismo rector externo preexistente que pueda asumir esa función sin distorsionar su misión propia. Por esa razón, su conducción recae directamente en la SIDE a través de una Dirección de Inteligencia Científico-Técnica creada en su interior, con personal especializado y vínculos formalizados con los organismos que integran el subsistema. Esta solución evita la creación de una nueva burocracia y garantiza que la articulación entre el conocimiento científico-técnico y las prioridades estratégicas del sistema ocurra en el nivel más próximo a la conducción.

El SITEC articula la información producida por los organismos científico-técnicos, las sociedades del Estado y las empresas privadas con capacidades estratégicas: la Comisión Nacional de Energía Atómica (CNEA), la Comisión Nacional de Actividades Espaciales (CONAE), la Empresa Argentina de Soluciones Satelitales (ARSAT), el Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF), el Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), el Instituto Nacional de Tecnología Industrial (INTI), el Instituto

Nacional de Tecnología Agropecuaria (INTA), INVAP y Nucleoeléctrica Argentina. La relación del SITEC con estos organismos es de articulación informativa, no de conducción: no los subordina a lógicas de inteligencia ni interfiere en sus misiones propias, sino que integra y protege el conocimiento que producen en función de prioridades nacionales.

El subsistema se organiza en torno a tres ejes. El primero es el conocimiento del entorno estratégico: el SITEC produce inteligencia sobre el estado y la evolución de las capacidades tecnológicas de actores externos en sectores críticos para la Argentina: nuclear, espacial, alimentario, hídrico y minero, con particular atención a la extranjerización de la tierra, el litio y los recursos del subsuelo, y al posicionamiento de potencias extrarregionales sobre el Atlántico Sur, las Islas Malvinas, Georgias del Sur, Sandwich del Sur y los espacios marítimos circundantes. El segundo es la protección de activos soberanos: el SITEC detecta y analiza intentos de apropiación indebida de desarrollos nacionales, operaciones de captura tecnológica sobre organismos estratégicos e interferencias externas sobre infraestructuras críticas. El tercero es la orientación del desarrollo tecnológico soberano: la Dirección de Inteligencia Científico-Técnica de la SIDE articula ese conocimiento para ponerlo al servicio del proceso decisorio del Ejecutivo, operando como nexo entre la comunidad científico-técnica nacional y la conducción estratégica del Estado.

Subsistema Argentino de Inteligencia Integrada (SAII)

El Sistema de Inteligencia Nacional tiene componentes especializados, pero la información estratégicamente relevante para el Estado los desborda y en reiteradas oportunidades genera superposición de tareas. Organismos reguladores, fiscales, aduaneros, ambientales, financieros y provinciales producen y acumulan conocimiento que incide directamente sobre la seguridad nacional sin pertenecer formalmente al sistema. Incorporar a esos actores con criterios jurídicos claros para su participación, sin convertirlos en agencias de inteligencia, es la función que define al Subsistema Argentino de Inteligencia Integrada (SAII).

Bajo la conducción de la SIDE, el SAII amplía y cohesiona la comunidad de inteligencia nacional. El diseño del SAII toma como referencia la reforma del Sistema Brasileño de Inteligencia (SISBIN), que en 2023 reorganizó su arquitectura para resolver problemas que el sistema argentino también enfrenta: miembros heterogéneos sin criterios claros de adhesión y herramientas de coordinación insuficientes.

Para gestionar la diversidad de actores que componen el SAIL, el sistema los organiza según la naturaleza de su vínculo: organismos constitutivos, que integran el núcleo del sistema por mandato legal y misión institucional; organismos productores, que generan información estratégica desde sus propias funciones; organismos contribuyentes, que aportan conocimiento sectorial sin tener misión de inteligencia propia; y organismos provinciales, que desde su proximidad a los fenómenos producen información que el nivel nacional no puede capturar con la misma densidad, articulados mediante convenios voluntarios de adhesión aprobados por las legislaturas provinciales.

La integración del SAIL requiere una plataforma tecnológica que la sostenga: comunicación cifrada entre los miembros del sistema, una plataforma de gestión del conocimiento con rastreo y auditoría de accesos, y una base de datos integrada administrada por la SIDE.

Profesionalización

La formación profesional del personal de inteligencia constituye una prioridad transversal que tiende a ser sub abordada en términos de planificación. La Escuela Nacional de Inteligencia (ENI) debe operar como ámbito común de capacitación, certificación y actualización técnica para todos los subsistemas. Los programas de formación deberán incluir módulos sobre reunión y análisis de información, manejo de grandes volúmenes de datos, ciberespacio, amenazas híbridas, inteligencia artificial, relaciones internacionales, ética pública y derechos humanos, asegurando una cultura institucional alineada a valores del Estado democrático.

Se crearán instancias de formación superior validadas por la Comisión Nacional de Evaluación y Acreditación Universitaria (CONEAU).

A la vez se deberán estudiar modalidades exitosas que las principales escuelas de inteligencia del mundo llevan a cabo en materia de cooperación con otros servicios.

Control externo e interno, supervisión parlamentaria y auditoría de fondos reservados

El control del sistema de inteligencia debe ser nodal en la reforma, tanto como la arquitectura que se propone. De acuerdo con José Manuel Ugarte (1995), el control no debe ser entendido como una actividad intrínsecamente adversa a la actividad de inteligencia, destinada a limitarla, frustrarla, anularla y, en última instancia, suprimirla. El espíritu con que en esta materia debe ser ejercido es el

de conducir y encauzar la actividad hacia las metas fijadas por el poder político, evitando que se desvíe hacia otros fines y lesione aspectos de fundamental importancia para el Estado que la instituyó en su defensa, como son los derechos y garantías individuales.

La propuesta organiza el control en tres capas con funciones y objetos distintos, y en respuesta a una pregunta diferente: qué se va a hacer, qué se hizo y cómo se administraron los recursos.

Autorización *ex ante* y control *ex post*

La ausencia histórica de un mecanismo de autorización previa para el uso de capacidades intrusivas es una de las principales causas estructurales del abuso en el sistema de inteligencia argentino. Las reformas precedentes concentraron los esfuerzos en el control *ex post* —supervisión parlamentaria, auditoría de fondos— sin resolver el problema en su origen. La experiencia comparada muestra que otros sistemas consolidados resolvieron esta cuestión por vías distintas: Estados Unidos creó el Tribunal de Vigilancia de Inteligencia Extranjera (FISA Court), con competencia exclusiva para autorizar operaciones de vigilancia; España estableció un magistrado especializado del Tribunal Supremo con mandato de cinco años y plazo de respuesta de 72 horas; Alemania optó por una solución parlamentaria, radicando la autorización de medidas intrusivas en la Comisión G10 del Bundestag, un órgano especializado con acceso a material clasificado que opera con lógica técnica dentro del marco parlamentario. El Reino Unido desarrolló el Intelligence and Security Committee, con capacidad de revisión *ex ante* y acceso irrestricto a información sensible.

La propuesta, por lo tanto, es reformar la Comisión Bicameral de Fiscalización desdoblándola en dos salas con funciones diferenciadas. La primera, de autorización *ex ante*, estaría integrada por miembros técnicos no parlamentarios con mandatos fijos, escalonados y no renovables, designados por la Comisión Bicameral mediante un procedimiento que disocie la acreditación de idoneidad técnica de la negociación partidaria. Su función exclusiva sería autorizar previamente el uso de capacidades intrusivas, salvo en casos de urgencia debidamente fundados con ratificación posterior en plazo perentorio. La segunda sala mantendría la función de supervisión *ex post* que la Bicameral ya ejerce formalmente, fortalecida con personal técnico propio y con competencia explícita sobre el cumplimiento del Plan de Inteligencia Nacional (PIN). Este diseño no crea un organismo nuevo ni sale del marco parlamentario: amplía y especializa una estructura que ya existe, con rango legal propio y legitimidad democrática directa.

5. DOCTRINA

La doctrina es un conjunto de principios que le da sustento a una organización y a las acciones derivadas. Estos principios deben ser flexibles y estar sujetos a revisión, porque tienen que poder adaptarse al curso de los tiempos. El objetivo de una doctrina es definir la comprensión que la inteligencia argentina debe tener sobre su propia actividad con base en el Estado de derecho. Sin una doctrina propia desde los intereses nacionales, cada reforma se convierte en una reorganización formal: la historia del sistema de inteligencia argentino es, entre otras cosas, una historia de reformas carente de doctrina, ya que se cambian las estructuras, los nombres y las dependencias, pero nunca se responde el interrogante central de para qué existe el sistema.

Este apartado ofrece una aproximación de cuáles son los fundamentos que deben orientar la actividad de inteligencia en un Estado democrático que aspira a la soberanía, cuál es la concepción de amenaza que le corresponde, cuál es su relación con la sociedad a la que sirve y qué principios deben regular su conducta.

Inteligencia y democracia

El punto de partida de la doctrina es comprender que un Estado que renuncia a producir inteligencia soberana no elimina la inteligencia de su funcionamiento, la terceriza. Cuando el Estado carece de capacidad propia para interpretar su entorno estratégico, esa función es ejercida por otros actores —potencias externas, organismos multilaterales, consultoras privadas, agencias de inteligencia aliadas— cuyos intereses no coinciden necesariamente con los nacionales. La ausencia de inteligencia soberana contribuye de manera decisiva a la dependencia.

Desde esta perspectiva, la inteligencia es una función constitutiva del Estado soberano, no un instrumento de control político ni una herramienta de represión. Sus propósitos son la reducción de la incertidumbre que rodea las decisiones estratégicas del poder político democráticamente constituido y la identificación de oportunidades para el desarrollo del bien común.

A su vez, la actividad de inteligencia opera dentro de la Constitución y el secreto debe acotarse por el principio de proporcionalidad y sujeto a control. Esta subordinación es la condición que le permite operar con legitimidad en una democracia.

La legitimidad social como principio fundante

El sistema de inteligencia argentino debe construir un lazo de confianza con la sociedad mediante una reforma institucional que demuestre resultados concretos en nombre de la Nación. Esa confianza se acumula sobre la base de la cercanía y la continuidad, porque la legitimidad en el campo de la inteligencia es un capital frágil que puede tardar décadas en edificarse.

Para lograrlo resulta necesario instituir una dimensión formativa y pedagógica sostenida, orientada a comunicar cuáles son las amenazas que enfrenta el sistema democrático. Esa comunicación no expone operaciones ni revela fuentes, sino que construye gradualmente las condiciones para que la sociedad pueda distinguir entre un servicio legítimo y uno abusivo. En esa distinción reside la posibilidad de una delegación de confianza.

Definición soberana de amenazas

Uno de los sesgos más profundos del sistema de inteligencia argentino es la adopción acrítica de definiciones de amenaza construidas por actores externos. Las agendas del narcoterrorismo, el crimen organizado transnacional o la proliferación de armas de destrucción masiva no son categorías neutras: expresan las prioridades estratégicas de las potencias que las promovieron y los marcos conceptuales desde los que fueron formuladas. Adoptarlas sin mediación crítica implica una subordinación metodológica que orienta la actividad sin autonomía relativa.

La doctrina propone una definición soberana de amenazas que parta de los intereses nacionales y de una lectura propia del entorno estratégico. Esa definición reconoce amenazas en varias dimensiones:

Amenazas a la soberanía política y territorial: interferencias externas sobre el proceso decisorio del Estado, operaciones de desestabilización, presiones sobre el sistema judicial y político, y cualquier acción tendiente a condicionar la autonomía de las decisiones estratégicas nacionales.

Amenazas al orden constitucional: intentos de desestabilización del sistema democrático, operaciones de desinformación a escala, captura de instituciones del Estado por intereses privados o extranjeros, y cualquier acción que atente contra la continuidad del orden constitucional.

Amenazas a la defensa nacional: acciones de actores estatales y/o no estatales externos orientadas a comprometer la soberanía territorial, degradar las capacidades del sistema de defensa, proyectar poder militar sobre el espacio aéreo, marítimo o terrestre argentino. Esta dimensión incluye las operaciones

desarrolladas en el ciberespacio con potencial de afectar sistemas militares o infraestructura crítica, y las acciones propias de la zona gris, que son aquellas que operan por debajo del umbral del conflicto armado formal, pero condicionan la autonomía decisoria del Estado mediante amenazas híbridas de origen externo.

Amenazas a la seguridad interior: fenómenos de crimen organizado con capacidad de penetración institucional, economías ilegales con poder territorial, y operaciones de corrupción que capturen el proceso decisorio estatal en beneficio de intereses particulares.

Amenazas a los recursos estratégicos: procesos de apropiación o condicionamiento del acceso a recursos naturales críticos —agua, litio, hidrocarburos, tierra—, disputas de soberanía sobre el Atlántico Sur y la proyección antártica, y posicionamiento de actores extrarregionales en el entorno geopolítico inmediato.

Amenazas a la autonomía tecnológica: dependencia de infraestructura tecnológica externa en sectores estratégicos, operaciones de apropiación indebida de desarrollos científicos nacionales, y vulnerabilidades en los sistemas digitales del Estado.

Esta taxonomía no es exhaustiva ni cerrada. La definición de amenazas debe ser un proceso dinámico, revisado periódicamente por el Consejo de Inteligencia Nacional sobre la base de los análisis del sistema y de la evolución del entorno estratégico.

Principios doctrinarios

Los principios doctrinarios son los fundamentos que orientan la actividad de inteligencia y funcionan como criterios comunes para el diseño de procedimientos, la evaluación del personal y el control de la gestión.

Legalidad y proporcionalidad: toda acción de inteligencia debe estar habilitada por la ley y limitada al mínimo necesario para cumplir su objetivo.

Oportunidad y objetividad: la información producida debe ser oportuna, verificable y ajena a cualquier sesgo sectorial o partidario. El sistema debe producir lo que el Estado necesita saber.

Protección de fuentes y medios: la seguridad del personal y de las capacidades técnicas constituye un interés estratégico del Estado. La exposición de fuentes o métodos compromete las operaciones y la capacidad del sistema.

Responsabilidad institucional: la inteligencia es un servicio público orientado a la preservación del bien común y de la soberanía nacional. La responsabilidad por las acciones del sistema recae en sus autoridades, sin excepción y sin posibilidad de exención por obediencia debida.

Subordinación democrática: el sistema opera bajo conducción política civil y está sujeto a control parlamentario. El secreto es una herramienta operativa y no debe regir como un principio de organización institucional.

La doctrina como proceso

El Decreto N° 1311/2015 representa el antecedente más sólido de construcción doctrinaria democrática en la historia del sistema de inteligencia argentino. Su contribución fue múltiple: publicó por primera vez la estructura orgánica del organismo, estableció un régimen de fondos que distinguía entre gasto público y reservado, implementó una metodología de trabajo por problemas que exigía autorización escrita y fundamentada para cada actividad, impulsó la profesionalización mediante escalafones diferenciados y formación obligatoria en la ENI, y transfirió las escuchas telefónicas al Ministerio Público Fiscal para garantizar control judicial. Fue, en síntesis, un esfuerzo genuino por dotar al sistema de transparencia, coherencia y subordinación democrática.

Esa experiencia es la que mejor ilustra por qué la doctrina debe entenderse como un proceso sostenido y no como un acto. La propuesta establece que la doctrina del Sistema de Inteligencia Nacional debe ser revisada periódicamente —con un ciclo no mayor a cuatro años— por el Consejo de Inteligencia Nacional, con participación de la ENI y de referentes académicos especializados. Si bien los principios son permanentes, las definiciones de amenaza y las prioridades estratégicas se actualizan con el entorno.

La doctrina debe tener además una dimensión formativa: debe ser conocida y apropiada por el personal del sistema. La ENI tiene en este punto una responsabilidad central: no solo transmitir técnicas, sino construir una cultura organizacional coherente con los principios que la sostienen. Finalmente, debe ser pública en sus fundamentos aunque reservada en sus aplicaciones operativas. Los ciudadanos tienen derecho a conocer el servicio que protege los intereses nacionales.

BIBLIOGRAFÍA

Libros y artículos académicos

Bobbio, Norberto (2014) *Democracia y secreto*. Editorial Fondo de Cultura Económica.

De Carvalho Rêgo, Eduardo y Justino de Oliveira, Gustavo (2023). Democracia defensiva na Alemanha e no Brasil na prática de hoje. *Seqüência: Estudos Jurídicos e Políticos*, UFSC. <https://periodicos.ufsc.br/index.php/sequencia/article/view/95761>

Damsky, José María (2019). *El pivote antártico*. Editorial Ciccus.

López Gobernado, Carlos (2019). Protegiendo la democracia alemana: Bundesamt für Verfassungsschutz (BfV). *Quadernos de criminología: revista de criminología y ciencias forenses* N° 46 (4-6) <https://dialnet.unirioja.es/servlet/articulo?codigo=7162719>

Poczynok, Iván (2023). Política y servicios de inteligencia: hoja de ruta para un sistema legítimo y efectivo. Fundar.

Sain, Marcelo (2016). *La casa que no cesa. Infortunios y desafíos en el proceso de reforma de la ex SIDE*. Editorial Octubre.

Sain, Marcelo (1997). Condiciones institucionales del control parlamentario de las actividades y organismos de inteligencia del estado. En *Seminario Control democrático en los organismos de seguridad interior en la República Argentina*. Centro de Estudios Legales y Sociales [CELS]. <https://www.cels.org.ar/common/1997%2004%20Trabajo%20de%20Marcelo%20Sa%C3%ADn%20en%20el%20marco%20de%20Seminario%20sobre%20Control%20democratico.pdf>

Ugarte, José Manuel (1995). Inteligencia y democracia. *Nueva Sociedad*. https://static.nuso.org/media/articles/downloads/2439_1.pdf

Ugarte, José Manuel (2012). *El control público de la actividad de inteligencia en América Latina*. Editorial Ciccus.

Fuentes normativas

Decreto N.° 1311/2015.

Decreto N.° 52/2019.

Decretos N.° 614 y 615/2024.

Decreto N.° 941/2025.

Decreto N.° 950/2024.

Decreto N.° 11.693 (2023). Reorganización del Sistema Brasileiro de Inteligência (SISBIN). Presidência da República. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm

Decreto 338 de 2022. Presidencia de la República de Colombia.

Documento CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa (2011). Departamento Nacional de Planeación de la República de Colombia.

Foreign Intelligence Surveillance Act [FISA] (1978). United States Congress.

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Ley G10) (1968). Bundestag.

Ley N.º 25.520 de Inteligencia Nacional (2001).

Ley N.º 27.126 (2015).

Ley Orgánica 2/2002, reguladora del control judicial previo del Centro Nacional de Inteligencia. Boletín Oficial del Estado. Reino de España. <https://www.boe.es/buscar/doc.php?id=BOE-A-2002-8627>

Ley 9/1968 de Secretos Oficiales. Boletín Oficial del Estado. Reino de España.

Reforma que fortalece y moderniza el Sistema de Inteligencia del Estado (2026). Ministerio del Interior de Chile. <https://www.interior.gob.cl/noticias/2026/01/28/congreso-des-pacha-a-ley-reforma-que-fortalece-y-moderniza-el-sistema-de-inteligencia-del-esta-do-tras-respaldo-del-ejecutivo/>

Fuentes institucionales

Agência Brasileira de Inteligência [ABIN] (2026). SISBIN: composición y atribuciones. <https://www.gov.br/abin/pt-br/institucional/sisbin>

Bundesamt für Verfassungsschutz [BfV] (2025). Verfassungsschutzbericht 2024. Ministerio Federal del Interior de Alemania. <https://www.verfassungsschutz.de>

Centro Nacional de Inteligencia de España [CNI] (2026). Controles. <https://www.cni.es/sobre-el-cni/controles>

Centro Nacional de Inteligencia de España [CNI] (2026). Oficina Nacional de Seguridad. <https://www.cni.es/oficina-nacional-de-seguridad>

Comando Conjunto de Ciberdefensa [CCCCD] (s.f.). Reseña histórica y funciones. Estado Mayor Conjunto de las Fuerzas Armadas de Argentina. <https://www.argentina.gob.ar/historia-del-comando-conjunto-de-ciberdefensa>

Grupo de Respuestas a Emergencias Cibernéticas de Colombia [CoCERT] (2026). *Informe de Tendencias de Amenazas Cibernéticas 2025*. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/433511>

Fuentes periodísticas

Agência Brasil (2023). Decreto presidencial define regras para atividades de inteligência.

Agência Brasil (2024). ABIN comemora 25 anos em meio à reforma do sistema de inteligência. <https://agenciabrasil.ebc.com.br/geral/noticia/2024-12/abin-comemora-25-anos-em-meio-reforma-do-sistema-de-inteligencia>

Aguilera, Edgardo (2025). Marcha atrás en licitaciones del Comando de Ciberdefensa. *Ámbito*. <https://www.ambito.com/politica/marcha-atras-licitaciones-del-comando-ciberdefensa-n6224116>

Dotson, Taylor (2025). In Defense of Democracy? *Taming Complexity*. <https://tamingcomplexity.substack.com/p/in-defense-of-democracy>

Duchiade, André. Agencia Brasileña de Inteligencia espío a periodistas durante gobierno de Bolsonaro. *LatAm Journalism Review*. <https://latamjournalismreview.org/es/articles/agencia-brasilena-de-inteligencia-espio-a-periodistas-durante-gobierno-de-bolsonaro-revelo-informe-de-la-policia/>

El Universo (2024). El escándalo de espionaje que involucra al expresidente Bolsonaro. <https://www.eluniverso.com/noticias/internacional/el-escandalo-de-espionaje-que-involucra-al-expresidente-bolsonaro-y-a-su-familia-en-brasil-nota/>

MinTIC (2026). Colombia fortalece su soberanía digital: durante 2025 logró reducir en un 48% los incidentes cibernéticos. <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/433511:Colombia-fortalece-su-soberania-digital-durante-2025-logro-reducir-en-un-48-los-incidentes-ciberneticos>

Motoryn, Paulo y Días, Tatiana (2023). Como o Brasil virou o paraíso da espionagem ilegal. *The Intercept Brasil*. <https://www.intercept.com.br/2023/10/28/brasil-virou-paraíso-da-espionagem-ilegal-com-michel-temer-jair-bolsonaro/>

The Economist (2026). Se avecina una revolución para los servicios de inteligencia de Alemania. *Infobae*. <https://www.infobae.com/economist/2026/04/03/se-avecina-una-revolucion-para-los-servicios-de-inteligencia-de-alemania/>