El Senado y la Cámara de Diputados de la Nación Argentina sancionan con fuerza de ley:

**PROYECTO DE LEY**

**SISTEMA INTEGRAL NACIONAL DE INTELIGENCIA (SINIRA)**

**Título I – Objeto y principios rectores**

**Artículo 1° – Objeto**.

Créase el Sistema Nacional de Inteligencia Integral de la República Argentina (SINIRA), en sustitución del régimen establecido por la Ley 25.520 y sus modificatorias, con el fin de garantizar la defensa nacional, la seguridad interior, la protección de los intereses estratégicos de la Nación y la preservación del orden constitucional, en el marco del respeto a los derechos y garantías establecidos por la Constitución Nacional y los tratados internacionales de derechos humanos ratificados por la República.

**Artículo 2° – Principios.**

El SINIRA se regirá por los principios de:

a) Supremacía constitucional y respeto irrestricto a los derechos humanos.

b) Control parlamentario riguroso y permanente.

c) Coordinación centralizada y ejecución descentralizada.

d) Legalidad, proporcionalidad y control judicial en toda actividad que afecte derechos individuales.

e) Transparencia institucional y rendición de cuentas.

## Título I BIS – Definiciones

**Artículo 2 bis – Inteligencia Exterior.**

Se entiende por Inteligencia Exterior la obtención, reunión, procesamiento, análisis y difusión de información relativa a actividades, capacidades o intenciones de actores estatales o no estatales en el ámbito internacional que puedan afectar la defensa nacional, la política exterior, la seguridad y los intereses estratégicos de la República Argentina.

**Articulo 2 ter- Inteligencia Estratégica Militar**

A los fines de la presente ley, se entiende por **Inteligencia Estratégica Militar** a la actividad sistemática y especializada de obtención, procesamiento, análisis y producción de información relativa a capacidades, recursos, doctrinas, intenciones y vulnerabilidades de actores estatales o no estatales que puedan afectar la defensa nacional. Su finalidad es apoyar la planificación, conducción y empleo de las Fuerzas Armadas en el nivel estratégico, coadyuvando a la formulación de la política de defensa y a la preservación de la soberanía, la integridad territorial y los intereses vitales de la Nación.

La Inteligencia Estratégica Militar se desarrollará con sujeción a la Constitución Nacional, las leyes vigentes, el principio de subordinación al poder civil y el respeto irrestricto de los derechos humanos.

**Artículo 2 quater – Inteligencia Interior.**

Se entiende por Inteligencia Interior la obtención, reunión, procesamiento, análisis y difusión de información relativa a amenazas, riesgos o actividades ilícitas que se desarrollen dentro del territorio nacional y que afecten la seguridad interior, el orden constitucional, la vigencia del estado de derecho y la integridad de las instituciones

democráticas.

En ningún caso podrá comprender actividades de vigilancia o espionaje sobre personas, partidos políticos, organizaciones sociales, sindicales, religiosas o empresariales por razones de ideología, pertenencia lícita o ejercicio de derechos constitucionales.

**Artículo 2 quinquies – Ciber inteligencia.**

Se entiende por Ciberinteligencia el conjunto de actividades destinadas a prevenir, detectar, neutralizar y responder a amenazas provenientes del ciberespacio que afecten la seguridad nacional, la infraestructura crítica, los sistemas de defensa, las redes de comunicaciones, la economía digital y la soberanía tecnológica de la República Argentina.

Incluye la protección de datos sensibles del Estado, la prevención de ciberataques, la detección de operaciones de influencia y el resguardo de la integridad de los procesos democráticos.

## Título II – Organización del SINIRA

**Artículo 3° – Componentes.**

El SINIRA estará conformado por:

a) Dirección Nacional de Inteligencia Exterior (DNIEX)

b) Dirección Nacional de Inteligencia Militar (DNIM)

c) Dirección Nacional de Inteligencia Criminal Interior (DNICI)

d) Dirección Nacional de Ciberinteligencia (DNCIBER)

e) La Unidad de Información Financiera (UIF), conforme Ley 25.246, con autonomía técnica y funcional.

f) Las dependencias de inteligencia criminal de las Fuerzas Policiales y de Seguridad Federales, bajo coordinación de la DNICI.

g) Las dependencias de inteligencia criminal de policías y fuerzas de seguridad

subnacionales, bajo control judicial y en cooperación con la DNICI.

h) El Consejo Nacional de Inteligencia (CNI).
i) El Órgano Técnico Permanente de Inteligencia (OTPI).
**j)** El Instituto Nacional de Inteligencia (INI).

**Artículo 4° – Dirección Nacional de Inteligencia Exterior (DNIEX).**
La Dirección Nacional de Inteligencia Exterior tiene por misión la obtención, análisis y producción de información relativa a amenazas y riesgos que afecten la seguridad y los intereses estratégicos de la Nación en el ámbito internacional. Dependerá funcional y orgánicamente en el Ministerio de Relaciones Exteriores, Comercio y Culto. El Poder Ejecutivo Nacional será quien designe su titular.

**Artículo 5°- Dirección Nacional de Inteligencia Militar (DNIM)**
La Dirección Nacional de Inteligencia Militar tiene por misión planificar, dirigir y coordinar la actividad de inteligencia de las Fuerzas Armadas, a fin de obtener, procesar, analizar y producir información necesaria para la defensa nacional, en el nivel estratégico, operacional y táctico, conforme a la Política de Defensa y a la conducción superior del Estado.

**Artículo 6° – Dirección Nacional de Inteligencia Interior y Criminal (DNICI).**
La Dirección Nacional de Inteligencia Interior y Criminal tendrá a su cargo la inteligencia sobre amenazas internas, incluyendo terrorismo, crimen organizado, delitos federales complejos, ciberdelitos y contrainteligencia. Toda actividad que afecte derechos ciudadanos deberá realizarse bajo control judicial. Dependerá funcional y

orgánicamente en el Ministerio de Seguridad Nacional. El Poder Ejecutivo Nacional será quien designe su titular

**Artículo 7° – Dirección Nacional de Ciberinteligencia (DNCIBER).**
Será responsable de la protección de infraestructura crítica digital, la ciberseguridad nacional y la inteligencia de señales. El Poder Ejecutivo Nacional será quien designe su titular.

**Artículo 8 – Instituto Nacional de Inteligencia (INI).**
Créase el Instituto Nacional de Inteligencia (INI), como organismo rector en materia de formación, capacitación y perfeccionamiento de los agentes de inteligencia de todas las agencias integrantes del SINIRA.
El INI tendrá a su cargo:
a) La instrucción básica y avanzada de los agentes en inteligencia estratégica, inteligencia táctica, contrainteligencia, inteligencia de señales, ciberinteligencia y delitos federales complejos.
b) El diseño y ejecución de programas de actualización permanente en coordinación con el Órgano Técnico Permanente de Inteligencia (OTPI) y las agencias especializadas.
c) La cooperación académica y técnica con universidades nacionales, centros de investigación y organismos internacionales, en el marco de convenios autorizados por el Consejo Nacional de Inteligencia (CNI).
d) La elaboración de manuales doctrinarios y protocolos de actuación uniformes para la comunidad de inteligencia.
La dirección del INI será ejercida por un funcionario designado por el Poder Ejecutivo Nacional, con rango equivalente al de Subsecretario de Estado.

**Artículo 9° – Unidad de Información Financiera (UIF).**

Se integra al SINIRA con autonomía técnica, con misión de detección, prevención y análisis de operaciones de lavado de dinero, financiamiento del terrorismo y delitos financieros.

## Título III – Consejo Nacional de Inteligencia y OTPI

**Artículo 10° – Consejo Nacional de Inteligencia (CNI).**

Será el máximo órgano de coordinación del SINIRA, integrado por: presidente de la Nación, Ministros de Relaciones Exteriores, Defensa, Seguridad, Justicia y el Director Ejecutivo de la UIF.

**Artículo 11° – Funciones del CNI.**

Definir prioridades estratégicas de inteligencia, aprobar planes anuales y coordinar a las agencias del sistema.

**Artículo 12° – Órgano Técnico Permanente de Inteligencia (OTPI).**

Será un organismo asesor interministerial y multisectorial de expertos civiles y militares, encargado de evaluaciones estratégicas y coordinación técnica.

## Título IV – Inteligencia Criminal y jurisdicción subnacional

**Artículo 13° – Facultades.**

Las fuerzas policiales y de seguridad subnacionales podrán realizar inteligencia criminal en el marco de investigaciones judiciales y prevención estratégica.

**Artículo 14° – Control judicial.**

Las tareas de inteligencia criminal deberán desarrollarse bajo estricto control judicial federal o jurisdiccional.

**Artículo 15° – Coordinación federal.**

La información de inteligencia criminal producida en provincias deberá compartirse en el CNI si implica riesgos al orden constitucional, estado de derecho o seguridad nacional.

## Título V – Personal de inteligencia

**Artículo 16° – Ingreso.**

El personal será incorporado mediante concurso público con carácter reservado, con paso obligatorio en el Instituto Nacional de Inteligencia (INI) para su formación en la especialidad que ha sido incorporado.

**Artículo 17° – Declaraciones juradas.**

Todo el personal deberá presentar declaraciones juradas de bienes patrimoniales conforme Ley 25.188 y Ley 26.857.

**Artículo 18° – Reserva de identidad.**

La identidad reservada será excepcional y solo aplicable a tareas cuya naturaleza lo requiera estrictamente. Los cargos de conducción tendrán identidad pública.

**Artículo 19° – Obediencia debida.**

La obediencia debida no podrá ser alegada como eximente de responsabilidad en caso de violaciones de derechos o comisión de delitos.

**Artículo 20° – Régimen de secreto.**

Los integrantes de los organismos de inteligencia, legisladores de la Comisión Bicameral, autoridades judiciales y demás funcionarios que accedan a información clasificada deberán guardar el más estricto

secreto y confidencialidad, incluso tras el cese de funciones. La violación será penada conforme Código Penal (arts. 222 y 223).

## Título VI – Control y supervisión

**Artículo 21° – Control parlamentario.**

La Comisión Bicameral de Fiscalización de Organismos de Inteligencia tendrá acceso pleno a documentación clasificada, citación obligatoria de funcionarios y control presupuestario.

**Artículo 22° – Control judicial.**

Toda actividad de inteligencia que implique restricciones a derechos constitucionales requerirá autorización judicial previa y control posterior.

## Título VII – Información, archivos y desclasificación

**Artículo 23° – Clasificación.**

La información producida se clasificará en Secreta, Confidencial o Pública.

**Artículo 24° – Desclasificación.**

La información clasificada tendrá un plazo mínimo de desclasificación de veinte (20) años, salvo disposición fundada del Poder Ejecutivo.

**Artículo 25° – Protección de datos.**

Se aplicará la Ley 25.326. Prohíbese almacenar datos por razones de raza, religión, ideología, pertenencia a organizaciones lícitas o actividades privadas.

**Artículo 26° – Archivos.**

Los organismos deberán centralizar sus archivos en un Banco de Protección de Datos de Inteligencia. Datos irrelevantes deberán ser destruidos.

## Título VIII – Interceptaciones de comunicaciones

**Artículo 27° – Interceptaciones.**

La Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado, dependiente de la Corte Suprema de Justicia de la Nación, es el único órgano autorizado para ejecutar interceptaciones ordenadas judicialmente.

## Título IX – Fondos de inteligencia

**Artículo 28° – Publicidad.**

Las partidas presupuestarias de inteligencia serán públicas, salvo aquellas estrictamente reservadas por razones de seguridad nacional.

**Artículo 29° – Control de fondos.**

Los fondos reservados estarán sujetos al control de la Comisión Bicameral y a los mecanismos de auditoría de la Ley 24.156.

**Artículo 30° – Transparencia.**

Los organismos deberán rendir cuentas de los fondos reservados preservando la seguridad operativa.

## Título X – Sanciones y penalidades

**Artículo 31 – Ámbito de aplicación.**

Las conductas tipificadas en este Título se considerarán **agravantes funcionales** de los delitos previstos en el Código Penal de la Nación, cuando fueran cometidas por funcionarios o agentes de los organismos de inteligencia en ejercicio o con motivo de sus funciones.

En tales casos, las penas establecidas en los artículos siguientes se aplicarán **sin perjuicio** de las sanciones generales previstas en el Código Penal, y prevalecerán en cuanto resulten más gravosas.

**Artículo 32 – Espionaje interno ilegal.**

Será penado con prisión de tres (3) a diez (10) años e inhabilitación perpetua el agente que, fuera de los casos autorizados judicialmente, realice espionaje sobre partidos políticos, organizaciones sociales, sindicales, religiosas, empresariales, periodistas, magistrados o personas por motivos ideológicos, de opinión política o ejercicio de derechos constitucionales.

**Artículo 33 – Espionaje contra autoridades.**

Será penado con prisión de cinco (5) a quince (15) años e inhabilitación perpetua el agente que realice espionaje contra autoridades constitucionales, candidatos a cargos electivos, jueces o miembros de las Fuerzas Armadas o de Seguridad.

**Artículo 34 – Inteligencia contra la seguridad nacional.**
Será penado con prisión de diez (10) a veinte (20) años y pérdida definitiva de jubilación o retiro el agente que realice actividades ilegales que afecten la seguridad nacional, el orden democrático o la división de poderes.

**Artículo 35 – Interceptaciones ilegales.**
Será penado con prisión de tres (3) a diez (10) años el funcionario que, sin orden judicial, intercepte comunicaciones o acceda a documentos privados, físicos o digitales, cualquiera sea su soporte o formato.

**Artículo 36 – No destrucción de registros.**
Será penado con prisión de dos (2) a seis (6) años el funcionario que omita destruir registros, copias o archivos de comunicaciones interceptadas judicialmente, una vez cumplido el objeto procesal de la medida.

**Artículo 37 – Incumplimiento de normas de relación.**
Será penado con prisión de seis (6) meses a tres (3) años el funcionario que incumpla las normas de actuación institucional y de relación interorgánica previstas en esta ley.

**Artículo 38 – Acciones prohibidas.**
Será penado con prisión de tres (3) a diez (10) años el funcionario o ex agente que realice actividades de inteligencia prohibidas por las leyes 23.554, 24.059 y por la presente ley.

## Título XI – Disposiciones finales

**Artículo 39° – Derogación.**

Deróganse la Ley 25.520, la Ley 27.126 y toda norma complementaria.

**Artículo 40° – Transición.**

El Poder Ejecutivo dispondrá en un plazo de 180 días la reorganización institucional, administrativa y presupuestaria del SINIRA.

**Artículo 41° – Vigencia.**

La presente ley entrará en vigor desde su publicación en el Boletín Oficial.

**Firmante:** Gerardo Milman.

**Fundamentos:**

Señor presidente;

El presente proyecto de ley para la creación de un **Sistema Nacional de Inteligencia Integral (SNII)** surge de la necesidad impostergable de adecuar el marco institucional argentino a los desafíos de seguridad del siglo XXI.

La historia reciente de nuestro país demuestra que el sistema de inteligencia vigente ha sido **ineficaz para prevenir amenazas estratégicas** y, en ocasiones, se ha desviado hacia prácticas de espionaje interno con fines políticos, vulnerando derechos fundamentales.
La falta de coordinación entre agencias, la escasa profesionalización de su personal y la ausencia de un verdadero control parlamentario y judicial han debilitado la confianza de la ciudadanía en el sistema.

Estamos siendo testigos directos que el mundo actual está atravesando una transformación acelerada. Tras el colapso de la Unión Soviética, el orden internacional experimentó un breve período unipolar dominado por los Estados Unidos. Sin embargo, en las últimas dos décadas emergió una competencia estratégica con **China**, que dio lugar a una lógica bipolar, para finalmente evolucionar hacia un **escenario multipolar** con múltiples actores de peso**: India, Rusia, Turquía, Japón, Irán, Arabia Saudita, Israel, la Unión Europea, Brasil**, entre otros, que ponen en

discusión sobre la gran hegemonía y la diversidad de competencias estratégicas entre potencias emergentes.

Estamos asistiendo a un conflicto bélico como es la invasión rusa a Ucrania, con más de tres años de duración, con serio riesgo de propagarse hacia otros países europeos, que conllevaría al involucramiento de la OTAN, con todo lo que implicaría en términos militares, geopolíticos y comerciales que impactarían a nivel mundial.

Este **nuevo equilibrio inestable** genera tensiones permanentes en el comercio internacional, la seguridad energética, la disputa tecnológica y la hegemonía en organismos multilaterales. La Argentina no puede permanecer al margen de este reordenamiento global: requiere un sistema de inteligencia con visión estratégica para anticipar los riesgos y oportunidades que se derivan de la transición hacia un mundo multipolar.
Las guerras contemporáneas trascienden el campo de batalla convencional, en la actualidad, las amenazas son **híbridas**: se combinan

ciberataques, campañas de desinformación, manipulación de infraestructuras críticas, operaciones de influencia y crimen organizado transnacional.

Los **delitos cibernéticos de avanzada** –robo de datos estratégicos, hackeo a sistemas financieros, ataques a servicios públicos esenciales, sabotajes informáticos, afectación que atenten contra la confidencialidad, integridad o disponibilidad de sistemas, redes, datos o servicios, incluyendo el phishing, el ransomware, el malware financiero, el uso malicioso de tecnologías deepfake o de inteligencia artificial generativa, y la manipulación o sustracción de datos biométricos, entre algunos de los delitos informáticos que ponen en jaque la seguridad nacional y económica.
La Argentina necesita contar con un **área específica de ciberinteligencia**, coordinada con Defensa, Seguridad y la Unidad de Información Financiera, para proteger tanto al Estado como al sector privado de estas amenazas.

Asimismo, en nuestra región está atravesada por fenómenos criminales de gran magnitud. América del Sur concentra los principales países productores de cocaína y marihuana, al tiempo que crece la producción y tráfico de **drogas sintéticas y opioides** como el fentanilo, con consecuencias devastadoras para la salud pública.

Según la **Oficina de las Naciones Unidas contra la Droga y el**

**Delito** (**ONUDD** o **UNODC) l**a **producción de cocaína alcanzó un récord histórico en 2023**, con **3.708 toneladas**, un aumento del **34 % respecto a 2022**, impulsada por la expansión de cultivos en Colombia y mejoras en rendimiento. (UNODC, *World Drug Report 2025*).
Se resalta que Colombia concentra el **67 % de los cultivos ilícitos de coca** y registró un **53 % de incremento en la producción de cocaína en 2023**, con incautaciones nacionales récord de **960 toneladas en 2024**. (UNODC).
Por otro lado, en América Latina se observa un **crecimiento sostenido de los decomisos** de cocaína y drogas sintéticas, acompañados de un aumento en la violencia y la consolidación de **organizaciones criminales transnacionales**.

Según informes de Europol, el **68 % de las redes criminales más peligrosas son transnacionales**, con operaciones que conectan América Latina, Europa y África.
El **36 % de estas redes se dedica al narcotráfico** y el **32 % al lavado de**

**dinero**, infiltrándose en la economía legal a través de empresas fachada (transporte, comercio agrícola, servicios).

Para el año 2023, en cooperación con Eurojust y países de la región, se decomisaron drogas en la UE por un valor estimado de **25.600 millones de euros**, más del doble que en 2022.
Recientes casos confirman la **conexión directa entre redes latinoamericanas y europeas**, utilizando puertos estratégicos (Rotterdam, Amberes, Valencia) y centros logísticos en América del Sur. ( Europol – *Serious and Organised Crime Threat Assessment (SOCTA) 2024)*

El **narcotráfico no actúa en soledad**: converge con el terrorismo internacional, la trata de personas y el tráfico de armas, en redes criminales que financian actividades ilícitas globales. La infiltración en economías locales, la corrupción de instituciones y la violencia urbana son efectos palpables que también impactan en nuestro país.

Por su parte, la amenaza que representan las organizaciones criminales transnacionales en América Latina exige un abordaje integral desde el Estado argentino. En la actualidad, grupos como **Los Choneros** y **Los Lobos** en Ecuador, el **Comando Vermelho** y el **Primer Comando da Capital (PCC)** en Brasil, y el **Tren de Aragua** de origen venezolano, se han consolidado como verdaderos

actores no estatales con capacidad de desestabilización regional.

Vale enfatizar sobre el crecimiento exponencial de estas estructuras criminales que responde a varios factores: la expansión del mercado global de cocaína, el incremento del tráfico de drogas sintéticas, la permeabilidad de las fronteras, la

debilidad de las instituciones estatales en algunos países de la región y la existencia de extensas zonas donde la presencia estatal es mínima o inexistente.

Estas organizaciones no solo controlan economías ilícitas, sino que ejercen **poder territorial efectivo**, particularmente en puertos estratégicos, corredores logísticos y centros urbanos vulnerables.

En el caso de **Los Choneros** y **Los Lobos**, el control de los puertos ecuatorianos de Guayaquil y Esmeraldas los ha convertido en actores clave del tráfico de cocaína hacia Europa, esto ha generado que la tasa

de homicidios pasara de más de 6 homicidios cada 100.000 habitantes a tener la más alta en 2023 en 45 homicidios por cada cien mil habitantes.

En Brasil, el **PCC** y el **Comando Vermelho** se han expandido más allá de las fronteras nacionales, penetrando en Bolivia, Paraguay y Argentina para garantizar el abastecimiento de cocaína y el control de rutas hacia el Atlántico y África.

El **Tren de Aragua**, por su parte, se ha transformado en el fenómeno criminal más expansivo de los últimos años. Nacido en las cárceles de Venezuela, hoy opera en al menos siete países sudamericanos, diversificando sus actividades hacia la trata de personas, la explotación de migrantes, la minería ilegal, la extorsión y el narcotráfico. Su capacidad de movilidad transfronteriza y su brutalidad en la ejecución lo convierten en un factor de inestabilidad creciente.

Además, hay que destacar que el **Cártel de los Soles**, es una organización criminal venezolana vinculada al narcotráfico, la corrupción estatal y el lavado de activos. Tanto la administración del presidente estadounidense, Donald Trump, como el presidente argentino, Javier Milei, han señalado como grupo terroristas al Cartel de los Soles.
Nuestro país lo incorporo al Cartel de los Soles en el Registro Público de Personas y Entidades vinculadas a Actos de Terrorismo y su Financiamiento (RePET) en el corriente año. Su estructura transnacional y sus nexos con otros cárteles latinoamericanos lo convierten en un actor de riesgo estratégico para la región y el Cono Sur.

Estas dinámicas configuran una **amenaza híbrida** para la seguridad de los Estados y la estabilidad democrática de la región. No se trata únicamente de bandas criminales aisladas, sino de estructuras organizadas con **capacidad financiera, armada y logística** para desafiar la autoridad estatal, corromper instituciones, infiltrar circuitos económicos legales y consolidar su influencia en territorios estratégicos.
La consecuencia directa de esta expansión es la **erosión del monopolio estatal de la fuerza**, el aumento sostenido de los índices de homicidios, la fragilización del control penitenciario, el debilitamiento de la confianza en las instituciones y el riesgo de que estos grupos avancen en **alianzas con organizaciones terroristas internacionales o redes dedicadas al ciberdelito**.

En este contexto, la República Argentina no puede permanecer ajena. La creciente infiltración de estas organizaciones en el Cono Sur —particularmente del PCC, del Comando Vermelho y del Tren de Aragua—

obliga a fortalecer nuestras capacidades de **inteligencia, cooperación internacional, control fronterizo y articulación judicial**.

En el territorio argentino, la actuación de la **Resistencia Ancestral Mapuche (RAM)** y otras organizaciones vinculadas a agendas transnacionales plantea conflictos con la seguridad interior, con implicancias en materia de soberanía territorial y relaciones exteriores.

El Conflicto en Medio Oriente sus vinculaciones con el terrorismo internacional, donde el conflicto bélico entre Israel y la influencia del "**triple eje del mal**" (Hamás–Hezbollah–Irán) representan un foco de amenazas globales.

Estas organizaciones cuentan con antecedentes de operar en América Latina y con capacidad de financiamiento ilícito transnacional. La Argentina ya sufrió atentados vinculados al terrorismo internacional (Embajada de Israel en 1992 y AMIA en 1994), lo que refuerza la necesidad de inteligencia estratégica y mecanismos de prevención temprana. La falta de coordinación entre agencias y la debilidad de los sistemas de prevención resultaron en tragedias que marcaron a fuego la historia reciente.

Estos hechos deben ser recordados como prueba de la necesidad de una **inteligencia estratégica moderna, integrada y con control**

**democrático**, capaz de anticipar y neutralizar amenazas antes de que se materialicen.

Por otra parte es de vital importancia para la seguridad nacional, la debida prevención y protección de nuestra infraestructura critica de todo tipo de ataque, físico, o ciber, a nuestras centrales eléctricas, represas hídricas, yacimientos hidro carboníferos, redes de transporte vial, ferroviario y marítimo, los aeropuertos internacionales y nacionales, puertos, redes de suministro de agua potable, energía eléctrica, gasoductos, edificios gubernamentales, bases de datos estratégicos, sistema nacionales de salud, sectores de finanzas, defensa nacional, seguridad, para enumerar algunos.

El presente proyecto de ley se destaca por la inclusión en el sistema nacional de la **inteligencia financiera como pilar del sistema.** En el mundo desarrollado, los organismos de inteligencia financiera son **parte central del sistema de seguridad nacional**.

La incorporación de la **Unidad de Información Financiera (UIF)** al SNII –respetando su autonomía técnica y su función en la Ley 25.246– fortalece la lucha contra el financiamiento del terrorismo, el lavado de activos y la corrupción. Con ello, la Argentina se alinea con los estándares de la **Financial Action Task Force (FATF/GAFI)** y las prácticas de la Unión

Europea y Estados Unidos.

Se incorpora al proyecto la creación del **Instituto Nacional de Inteligencia (INI)**, como espacio de formación, capacitación y profesionalización permanente de los agentes de inteligencia.
La experiencia histórica argentina demuestra que uno de los mayores déficits del sistema ha sido la **falta de cuadros profesionales estables, especializados y con formación sistemática**, lo cual derivó en improvisación, dependencia política coyuntural y prácticas desviadas.

El nuevo Instituto permitirá **unificar criterios doctrinarios, establecer estándares profesionales y garantizar la capacitación continua** en áreas claves para la seguridad nacional: inteligencia estratégica, inteligencia táctica, contrainteligencia, inteligencia de señales, ciberinteligencia y delitos federales complejos.
En línea con las mejores prácticas internacionales —como la **CIA University** en Estados Unidos, la **Intelligence Academy** en Reino Unido o la **École du Renseignement** en Francia— el INI asegura que los agentes argentinos reciban una **formación técnica, ética y democrática**, adaptada a los desafíos del siglo XXI.

Además, mediante convenios con universidades, centros de investigación y organismos internacionales, se promueve la **transferencia tecnológica, la innovación académica y la cooperación internacional**, reforzando la interoperabilidad de nuestro sistema de inteligencia con países aliados.

En definitiva, el INI es un **pilar fundamental de la modernización del SINIRA**, al garantizar que sus recursos humanos cuenten con las competencias necesarias para anticipar y neutralizar amenazas complejas en un mundo multipolar, caracterizado por delitos transnacionales, guerras híbridas y ciberataques de creciente sofisticación.

Se busca desterrar el modelo de inteligencia al servicio de intereses partidarios, consolidando una estructura **al servicio de la Nación y bajo estricto respeto a los derechos humanos**.

Para asegurar un diseño eficiente y acorde a estándares internacionales, la iniciativa toma en consideración las experiencias de países con tradición de modernización de sus sistemas de inteligencia, que suelen ser destacados dentro la comunidad de inteligencia internacional.

Si tomamos el caso de los **Estados Unidos**, donde después de sufrir el 11-9, refundaron su sistema nacional de inteligencia, con la creación de la

figura del *Director of National Intelligence* (DNI) y la existencia de agencias especializadas (CIA, NSA, FBI) muestran la conveniencia de una coordinación centralizada con agencias operativas y de ciberinteligencia fuertes, así como la integración de la inteligencia financiera en ámbitos intersectoriales.

Si analizamos el sistema de inteligencia del **Reino Unido**, vemos una clara separación de funciones entre MI5 (seguridad interior), MI6/SIS (inteligencia exterior) y GCHQ (comunicaciones y ciberinteligencia), junto con el *Joint Intelligence Committee* como órgano técnico asesor, constituyen un modelo de especialización técnica unido a asesoramiento estratégico independiente.

Si nos vamos a la Europa continental, vemos que, en **Francia**, hallamos una distinción entre DGSE (inteligencia exterior) y DGSI (inteligencia interior), su dependencia ministerial combinada con canales de asesoramiento al Presidente y al Primer Ministro, y la articulación con unidades financieras (TRACFIN) muestran la importancia de agencias con perfil propio y coordinación política.

Mientras que, en **Alemania**, la combinación de BND (inteligencia exterior), BFV (protección de la constitución/inteligencia interior) y BSI (seguridad informática), junto a un sólido control parlamentario, ofrece lecciones sobre equilibrio entre eficacia y control democrático.

De todas esas experiencias se derivan principios operativos incorporados en el proyecto: agencias especializadas en inteligencia externa, inteligencia militar, inteligencia criminal, ciberinteligencia e inteligencia financiera (DNIEX, DNIM, DNICI, DNCIBER), un Órgano Técnico Permanente inspirado en el JIC británico para análisis estratégico independiente, integración de la UIF como FIU dentro del sistema y un régimen de control parlamentario y judicial reforzado.

El presente proyecto crea agencias especializadas con dependencia política ministerial, pero autonomía operativa:

**Dirección Nacional de Inteligencia Exterior (DNIEX)**, con mandato sobre amenazas internacionales; dependendiente del Ministerio de Relaciones Exteriores, Comercio y Culto.

**Dirección Nacional de Inteligencia Militar** (DNIM) con mandato para planificar, dirigir y coordinar la actividad de inteligencia de las Fuerzas Armadas, a fin de obtener, procesar, analizar y producir información necesaria para la defensa nacional, en el nivel estratégico, operacional y táctico de las fuerzas armadas.

**Dirección Nacional de Inteligencia Criminal Interior (DNICI),** como centro coordinador de inteligencia interna y criminal; las dependencias de inteligencia criminal federales, fuerzas de seguridad y policiales federales que reportan orgánica y funcionalmente a la ANII, garantizando centralización operativa y evitando solapamientos.
Asimismo, es dable destacar que se autoriza a las fuerzas policiales subnacionales a realizar actividades de inteligencia, siempre con el control judicial pertinente, y pueden asistir al ANICI siempre que haya alguna amenaza al orden constitucional, al estado de derecho o a la seguridad nacional.

**Dirección Nacional de Ciberinteligencia (DNCIBER),** con capacidades técnicas para detección, respuesta y análisis de amenazas en el ciberespacio.

La incorporación de la UIF al Sistema Integral Nacional de Inteligencia como inteligencia financiera permite articular la prevención financiera con la actividad de inteligencia, preservando la **autonomía técnica y funcional** que le confiere la Ley N° 25.246.

Este diseño busca equilibrio: centraliza el análisis, especializa la ejecución y preserva la responsabilidad federal, evitando una atomización que dificulte la eficacia.

La experiencia internacional demuestra que la eficacia en inteligencia no puede prescindir de controles democráticos.

El proyecto refuerza los siguientes instrumentos, el **control parlamentario**, aumentado para ello las facultades de la Comisión Bicameral de Fiscalización (acceso a clasificados, auditorías, control presupuestario y citación de funcionarios).

El debido **control judicial**, toda la actividad interna que restrinja derechos (intervenciones, escuchas, seguimientos) requiere autorización judicial

previa y control posterior, con procedimientos ágiles y garantías procesales estrictas. A su vez, se procura incrementar la transparencia selectiva, mediante la presentación de informes anuales con versiones no

clasificadas para la sociedad y versiones clasificadas para la Comisión Bicameral, equilibrando seguridad y rendición de cuentas.

Estas garantías buscan prevenir abusos, evitar la persecución política y recuperar la confianza pública en las instituciones de inteligencia.

Por otro lado, en el régimen sancionatorio, en el **artículo 31** deja claro que todas las sanciones son **agravantes específicas**. Así como desde los artículos **32 a 38** quedan reforzados como **delitos calificados** aplicables únicamente para los agentes de inteligencia.

La sofisticación del financiamiento ilícito y su estrecha vinculación con redes transnacionales obliga a incorporar a la **inteligencia financiera** en el diseño orgánico del sistema. La UIF aporta capacidades analíticas y acceso a reportes de operaciones sospechosas que resultan indispensables para desmantelar redes criminales y cortar el flujo financiero que las sostiene.

El crimen organizado y el terrorismo se financian cada vez más mediante mecanismos sofisticados. Entre los delitos más habituales se destacan, entre otros, el Lavado de dinero mediante **criptoactivos** y plataformas digitales, el uso de paraísos **fiscales** y **empresas offshore**, fraudes bancarios digitales, manipulación bursátil para blanquear capitales de origen criminal.

La incorporación se hace **respetando la autonomía técnica y la normativa vigente** (Ley 25.246), a fin de preservar independencia técnica, confidencialidad de las investigaciones y cumplimiento de estándares internacionales (GAFI/AML-CFT), evitando incumplir con la normativa internacional en la materia.

La derogación integral de la normativa anterior exige una transición técnica y administrativa que evite vacíos operativos. Por ello la ley prevé plazos y

mecanismos para que los organismos existentes mantengan funciones interinas mientras se instrumentan la reorganización, la reasignación presupuestaria y la capacitación del personal, siempre bajo control del

Congreso y con planes de implementación que garanticen continuidad operativa.

La reforma propuesta constituye una respuesta integral a los desafíos actuales: moderniza capacidades técnicas (ciber, señales, financiera), ordena y centraliza funciones para evitar dispersión y superposiciones, busca garantizar la eficiencia y eficacia del sistema integral de inteligencia nacional, integra la agenda federal con la coordinación central y garantiza mecanismos robustos de control democrático y judicial siguiendo los estándares de los países más avanzados en la materia.

Se trata de dotar a la República Argentina de un sistema de inteligencia **efectivo, profesional, transparente y sujeto a la Constitución**, capaz de proteger la soberanía y la seguridad ciudadana en un mundo cada vez

más complejo y multipolar.

Nuestro país enfrenta un contexto internacional y regional signado por la complejidad, la volatilidad y la convergencia de amenazas híbridas, criminales y terroristas. La experiencia histórica de nuestro país, sumada al diagnóstico del presente, obliga a diseñar un **nuevo sistema de inteligencia integral**, federal, moderno y democrático.

El presente proyecto de ley busca responder a ese desafío, dotando a la República de un sistema alineado con los mejores estándares internacionales, pero adaptado a nuestra realidad. Con ello, se sientan las bases para un Estado más fuerte, soberano y capaz de proteger a sus ciudadanos frente a los riesgos del siglo XXI.

Por todo lo expuesto, sometemos a la consideración del Honorable Congreso de la Nación la aprobación del presente proyecto de ley.

**Firmante:** Gerardo Milman.