DIPUTADOS
ARGENTINA

"2025 -AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA"

P R O Y E C T O DE LEY

EL SENADO Y LA CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA

REUNIDOS EN CONGRESO SANCIONAN CON FUERZA DE LEY

CREACIÓN DEL "CONSEJO FEDERAL DE INFRAESTRUCTURAS ESTRATÉGICAS YCRÍTICAS (COFIEC)."

CAPÍTULO I: Objeto y Finalidad

Artículo 1°. Objeto de la Ley

La presente ley tiene como objeto crear el Consejo Federal de Infraestructuras Estratégicas y Críticas (COFIEC) para la identificación, clasificación y protección de las Infraestructuras Estratégicas y Críticas de la Nación, con especial enfoque en la seguridad nacional y la colaboración federal.

CAPÍTULO II: Creación y Dependencia

Artículo 2°. Creación y Dependencia

Créase el Consejo Federal de Infraestructuras Estratégicas y Críticas (COFIEC) como órgano de asesoramiento y coordinación en el ámbito del Poder Ejecutivo Nacional y bajo la supervisión del Congreso de la Nación.

CAPÍTULO III: Composición y Organización

Artículo 3°. Composición

El COFIEC estará compuesto por:

1. **Consejo Ejecutivo**
   i. **Presidente** designado por el Ministerio de Defensa de la Nación,
   ii. **Vicepresidente** por el Ministerio de Seguridad Nacional y,
   iii. **VocalTitular**por la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete de Ministros de la Nación.

Los cargos directivos deberán ser cubiertos por profesionales idóneos con experiencia comprobable en gestión de infraestructuras o seguridad nacional.

2. **Representantes de Ministerios de la Nación**

Un representante técnico de cada Ministerio, Secretaría de Estado u Organismo nacional relacionado con sectores estratégicos y críticos (energía, transporte, comunicaciones, etc.),

i. Los profesionales deberán contar con matrícula habilitante vigente en disciplinas directamente vinculadas a la actividad objeto de análisis, tales como ingeniería, arquitectura, ciencias aplicadas u otras afines. Asimismo, deberán acreditar experiencia específica en el estudio, diseño, gestión o protección de Infraestructuras Estratégicas y Críticas.

3. **Comité Federal Consultivo**

Integrado por 1 (uno)representante de cada una de las provincias de nuestro país y de la Ciudad Autónoma de Buenos Aires, designados por sus respectivos gobiernos,

i. Deberán acreditar conocimientos en planificación territorial o gestión de riesgos.

4. **Comité Técnico-Científico**

Estará conformado por **profesionales con trayectoria comprobada** en el **diseño, construcción, operación y evaluación de la resiliencia** de **infraestructuras estratégicas y críticas**, garantizando un enfoque técnico sólido en la materia,

i. Los integrantes serán **propuestos por los Consejos Profesionales** con competencia a nivel nacional en **Ingeniería, Arquitectura** u otras disciplinas vinculadas a la temática regulada. Para su incorporación, será requisito contar con **matrícula profesional vigente**, con alcance **nacional o provincial**, conforme a la especialidad y ámbito de análisis correspondiente,

ii. El Comité también contará con **consejeros de carácter consultivo**, provenientes de **Academias Nacionales de Ingeniería y Ciencias, Universidades, asociaciones, cámaras del sector** y/o expertos del ámbito privado especializados en **infraestructura estratégica**, aportando conocimiento técnico y experiencia en la gestión y protección de instalaciones críticas.

Artículo 4°. Designación y Duración

Los cargos directivos serán designados por el Poder Ejecutivo Nacional con acuerdo del Congreso de la Nación, por un período de cuatro (4) años. Dichos miembros no percibirán remuneración adicional por sus funciones en el COFIEC, las cuales serán desempeñadas como parte de sus obligaciones institucionales dentro de los organismos públicos de origen.

En cuanto a la participación de asesores provenientes del sector privado, cuando su intervención sea requerida en virtud de sus competencias técnicas y profesionales específicas, los honorarios serán regulados de la siguiente manera:

i. Los honorarios profesionales serán financiados con cargo a las partidas presupuestarias de las instituciones públicas integrantes del COFIEC.
ii. Los montos, criterios de proporcionalidad y condiciones de contratación serán establecidos por la reglamentación que dicte la Autoridad de Aplicación, debiéndose garantizar que los honorarios no sean en ningún caso inferiores a los mínimos establecidos por los Consejos Profesionales con competencia en la materia.
iii. En todos los casos, los profesionales deberán contar con matrícula habilitante vigente y tramitar la correspondiente encomienda profesional ante el Consejo Profesional competente, conforme a las normas vigentes en la jurisdicción correspondiente.

CAPÍTULO IV: Funciones y Competencias

Artículo 5°. Funciones del COFIEC (Consejo Federal de Infraestructuras Estratégicas y Críticas)

El COFIEC tendrá las siguientes funciones primarias y específicas, estructuradas en tres ejes operativos:

1. **Identificación, Clasificación y Catalogación de Infraestructuras Estratégicas-Críticas**
   Establecer un Sistema Nacional de Identificación y Catalogación, con criterios técnicos unificados, que permita determinar el carácter estratégico y crítico de las infraestructuras a nivel nacional, provincial y local. Este sistema incluirá:
   i. Evaluación integral del impacto potencial de cada infraestructura sobre:

i. La Defensa y Seguridad Nacional
ii. La continuidad institucional del Estado
iii. La economía nacional y regional
iv. La salud pública y los servicios esenciales

ii. Análisis del grado de interdependencia con otros sistemas críticos, ya sean físicos, digitales o funcionales (por ejemplo: energía, agua, comunicaciones, transporte, defensa, ciberseguridad).

iii. Valoración de riesgos multidimensionales asociados a:
   i. Amenazas de origen natural (sismos, inundaciones, incendios, etc.)
   ii. Amenazas tecnológicas (fallas sistémicas, sabotaje técnico, etc.)
   iii. Amenazas deliberadas (terrorismo, sabotaje, ciberataques, intrusiones).

El proceso de clasificación se basará en los aportes técnicos del Comité Técnico-Científico, las recomendaciones del Comité Federal Consultivo, los dictámenes de los representantes de los Ministerios competentes, y será validado por el Comité Ejecutivo del COFIEC. La versión consolidada del Catálogo Nacional de Infraestructuras Estratégicas y Críticas deberá ser elevada al Congreso de la Nación para su registro y control parlamentario.

2. Protección Integral y Gestión del Riesgo

Desarrollar y coordinar políticas públicas para la protección física, digital y funcional de las infraestructuras catalogadas como estratégicas o críticas, incluyendo:

i. Elaboración y actualización de protocolos técnicos para la protección física (seguridad perimetral, control de accesos, blindaje estructural, etc.) y para la ciberseguridad (firewalls, segmentación de redes, detección de intrusiones, encriptación de datos, etc.), respetando estándares internacionales y regionales adaptados al marco jurídico argentino.
ii. Coordinación con gobiernos provinciales, municipios, entes autárquicos, empresas estatales y privadas operadoras de servicios estratégicos, para implementar Planes Integrales de Contingencia, Respuesta y Recuperación ante incidentes o amenazas que afecten la operatividad de las Infraestructuras Estratégicas y Críticas.

iii. Generación de un Sistema Nacional de Alerta Temprana y Monitoreo Continuo, que integre información proveniente de sensores físicos, sistemas SCADA, vigilancia remota y alertas de inteligencia cibernética.

3. **Desarrollo de Capacidades Técnicas y Fortalecimiento del Capital Humano** Promover la profesionalización, investigación y generación de conocimiento aplicado a la gestión de Infraestructuras Estratégicas y Críticas, mediante:

   i. El impulso de programas de formación específica en diseño, análisis de vulnerabilidades, gestión del riesgo y protección de infraestructuras estratégicas, en coordinación con universidades nacionales, centros de I+D y Consejos Profesionales de Ingeniería, Arquitectura, Seguridad, Ciberdefensa y disciplinas afines.
   ii. La institucionalización de un Sistema Nacional de Certificación de Competencias en Infraestructuras Estratégicas y Críticas, que garantice estándares de calidad y formación continua para técnicos, ingenieros, operadores y responsables de seguridad.
   iii. La suscripción de convenios de cooperación técnica y académica con organismos internacionales, redes científicas especializadas y organismos multilaterales, para fortalecer las capacidades nacionales en la materia.

<u>Artículo 6°</u>. Exposición de Resultados y Fiscalización del Desempeño

El COFIEC remitirá anualmente al Honorable Congreso de la Nación, un informe detallado sobre las actividades desarrolladas y los avances logrados, observando estrictamente los criterios de confidencialidad necesarios dada la naturaleza altamente sensible de la información involucrada, pues está vinculada a sistemas, servicios e instalaciones imprescindibles para el funcionamiento continuo del Estado, el normal desarrollo de las actividades económicas y sociales, y la preservación de la vida cotidiana. La revelación o uso indebido de estos datos podría comprometer la seguridad nacional y generar consecuencias graves, incluyendo el colapso de servicios esenciales o la interrupción de operaciones estratégicas de gran impacto colectivo.

CAPÍTULO V: Evaluación del COFIEC en Procesos de Privatización y Gestión de Infraestructuras Estratégicas y Críticas

Artículo 7°. Procedimiento para la Privatización y Gestión Privada

Toda decisión del Poder Ejecutivo de declarar "sujeta a privatización" o permitir la gestión privada de una empresa estatal con infraestructuras estratégicas y/o críticas debe cumplir con el siguiente procedimiento:

1. **Informe Previo**: El Poder Ejecutivo remitirá un informe al COFIEC que evaluará si la empresa o sus activos son estratégicos o críticos.
2. **Dictamen del COFIEC**: El COFIEC emitirá un dictamen vinculante en un plazo de 60 días hábiles, que podrá:
   i. **Autorizar la privatización de los activos** en caso de que se determine que no son estratégicos o críticos para la seguridad nacional.
   ii. **Aprobar la privatización con condiciones específicas,** estableciendo requisitos de seguridad y continuidad operativa que garanticen la protección de intereses estratégicos, cuando los activos presenten un valor relevante para la infraestructura nacional.
   iii. **Evaluar y proponer modelos de participación público-privada** en el desarrollo, operación y protección de infraestructuras esenciales para la seguridad nacional. Estas recomendaciones se emitirán cuando las circunstancias lo exijan, priorizando la sostenibilidad, eficiencia y resiliencia de dichas infraestructuras, con el fin de fortalecer las capacidades nacionales ante riesgos críticos y preservar los intereses estratégicos del país.

3. **Condiciones para la Gestión Privada**: La gestión privada de activos estratégicos o críticos estará sujeta al cumplimiento de las siguientes condiciones:
   i. **Control Estatal**: Supervisión directa del Estado, incluyendo la facultad de intervención en caso de riesgos para la seguridad nacional.
   ii. **Plan de Seguridad y Continuidad**: Obligación de presentar y mantener un plan exhaustivo de seguridad y continuidad operativa que garantice la protección y funcionalidad de los activos.

iii. **Veedores Estatales**: Participación obligatoria de representantes estatales en los directorios, para monitorear y asegurar el cumplimiento de los estándares de gestión.

iv. **Confidencialidad**: Implementación de protocolos estrictos para el manejo seguro de información crítica, resguardando su acceso y protección.

Artículo 8°. Criterios Generales para Evaluación de Activos

El COFIEC establecerá criterios para evaluar la vulnerabilidad y criticidad de los activos estratégicos, considerando factores de seguridad, defensa, impacto social, económico, ambiental y tecnológico.

CAPÍTULO VI: Definiciones

Artículo 9°. Definiciones

Para los fines de esta ley, se establecen las siguientes definiciones:

1. **Infraestructura Estratégica**: Conjunto de activos, instalaciones y sistemas clave cuya interrupción, daño o ataque comprometería gravemente el funcionamiento del Estado y la vida normal de la sociedad, afectando tanto la seguridad nacional como el desarrollo económico y social del país.

2. **Infraestructura Crítica**: Infraestructura esencial dentro de la categoría de infraestructura estratégica, cuyo funcionamiento continuo es imprescindible. Cualquier interrupción o destrucción de esta infraestructura tendría consecuencias graves e inmediatas para los servicios básicos y la población, sin soluciones alternativas factibles. Incluirá aquellas infraestructuras que, por su ubicación o función, sean esenciales en caso de emergencia o catástrofes naturales."

3. **Infraestructura Crítica Interprovincial**: Infraestructura situada en una o más provincias cuya perturbación o destrucción afectaría gravemente a dos o más provincias, requiriendo una coordinación interprovincial para su protección

4. **Infraestructura Condicionalmente Crítica:** Infraestructura cuyo carácter esencial varía según las condiciones temporales, emergencias o situaciones excepcionales. Aunque en situaciones normales no es considerada ni crítica ni estratégica, bajo ciertos escenarios (desastres naturales, conflictos, pandemias o eventos que alteren el entorno habitual) puede volverse indispensable para la continuidad de servicios esenciales, la seguridad pública o la operatividad del Estado.

5. **Infraestructura de Conocimiento Crítico (ICC):** Conjunto de activos físicos y tecnológicos esenciales de carácter estratégico (como salud, energía, defensa o similares), cuya operación, mantenimiento continuo y restauración ante interrupciones o desastres dependen de manera crítica de conocimientos técnicos especializados, documentación técnica asociada y personal capacitado para su gestión. Donde el Estado deberá garantizar la preservación y disponibilidad permanente de dichos elementos, ante riesgos que comprometan la seguridad nacional, la provisión de servicios esenciales o la soberanía tecnológica.

6. **Servicio Esencial**: Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad y el bienestar socioeconómico de los ciudadanos, así como el eficaz funcionamiento de las instituciones del Estado.

7. **Sector estratégico:** Área diferenciada dentro de la actividad laboral, económica, cultural y productiva que proporciona un servicio esencial o garantiza el ejercicio de la autoridad del Estado y la seguridad interior, o que contribuye a la defensa nacional.

8. **Subsector estratégico:** Ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que establezca el COFIEC

9. **Zona crítica:** Zona geográfica donde están establecidas varias Infraestructuras Estratégicas y Críticas interdependientes, declarada como tal por el COFIEC para facilitar su protección y coordinación. Esta definición contempla y puede incluir a las infraestructuras criticas interprovinciales

10. **Operadores Críticos**: Entidades responsables públicas y-o privadas de la gestión y operación y mantenimiento de una infraestructura crítica.

11. **Análisis de riesgos**: Estudio de hipótesis de amenazas según escenarios para determinar y evaluar vulnerabilidades en los diferentes sectores estratégicos y las posibles repercusiones de su perturbación o destrucción.

12. **Infraestructura Estratégica Condicionalmente Crítica:** Caso particular que dada su importancia en situaciones de riesgo (como desastres naturales o conflictos), donde su pérdida afectaría no solo el paisaje urbano, sino también el patrimonio cultural y/o símbolo de la nación.

13. **Interdependencias:** Efectos que una perturbación en una infraestructura produciría en otras, considerando repercusiones en el propio sector, en otros sectores y a distintos niveles territoriales. Incluye coordinación de reuniones y

capacitaciones anuales para la actualización de mejores prácticas y respuestas ante incidentes.

14. **Protección de Infraestructuras Estratégicas y Críticas:**Conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las Infraestructuras Estratégicas y Críticas para prevenir, paliar y neutralizar daños causados por ataques, catástrofes naturales o accidentes. Esto incluirá protocolos de recuperación rápida en caso de incidentes que aseguren la continuidad de los servicios esenciales sin interrupciones graves. Asimismo, estas actividades comprenden el análisis permanente de riesgos y actualización de escenarios de amenaza, la implementación de medidas de seguridad físicas, tecnológicas y operativas, la coordinación entre instituciones públicas y privadas para una respuesta integrada ante crisis, la formación especializada del personal vinculado a estas infraestructuras y el desarrollo de capacidades de resiliencia, incluyendo redundancia técnica y planes de contingencia actualizados, con el fin de garantizar la operatividad de los servicios esenciales incluso en escenarios adversos..

15. **Información sensible:** Datos específicos sobre infraestructuras estratégicas que, de revelarse, podrían utilizarse para planear y ejecutar acciones que provoquen su perturbación o destrucción. El uso de esta información se restringe exclusivamente a fines de protección de Infraestructuras Estratégicas y Críticas.

CAPÍTULO VII: Identificación, Criterios y Responsabilidades

Artículo 10°. Identificación y Responsabilidad

El COFIEC elaborará y actualizará anualmente una lista de infraestructuras según las definiciones de esta ley. La responsabilidad de su protección será compartida entre el Estado Nacional, las Provincias y los operadores, en función de criterios de impacto humano, económico, ambiental, de seguridad, de estabilidad social, de confianza pública y de preservación de servicios esenciales y/o conocimientos tecnológicos estratégicos asociados a estos.

CAPÍTULO VIII: Coordinación Integral

Artículo 11°. Articulación Institucional

1. **Coordinación Nacional**: El COFIEC actuará como autoridad principal en la identificación y protección de las Infraestructuras Estratégicas y Críticas nacionales, estableciendo mecanismos eficaces de articulación con organismos técnicos especializados del ámbito nacional. Esta articulación incluirá el establecimiento de protocolos estandarizados, mecanismos seguros de intercambio de información sensible, la planificación conjunta de estrategias preventivas y respuestas coordinadas ante riesgos emergentes, así como la elaboración de planes integrales de contingencia. El objetivo primordial es asegurar una gestión integrada que fortalezca la resiliencia operativa y garantice la seguridad de las infraestructuras estratégicas.
2. **Coordinación Internacional**: El COFIEC analizará, dentro del marco legal argentino y mediante consultas previas con los actores involucrados, la conveniencia de cooperar con organismos internacionales dedicados a la protección de infraestructuras estratégicas. Esta cooperación se realizará únicamente cuando contribuya al fortalecimiento del conocimiento especializado nacional, la incorporación de estándares avanzados de seguridad cibernética, la transferencia tecnológica innovadora, y otras acciones que optimicen la resiliencia nacional, preservando siempre la soberanía tecnológica e intereses estratégicos del país.

CAPÍTULO IX: Información y Comunicación

Artículo 12°. Clasificación y Protección de Información

El COFIEC, en coordinación con la Secretaría de Inteligencia, establecerá niveles de clasificación para la información relacionada con las Infraestructuras Estratégicas y Críticas. Estos niveles serán revisados periódicamente, y se implementarán auditorías regulares sobre el acceso a dicha información clasificada, con el fin de prevenir filtraciones y garantizar la seguridad de los datos sensibles. Las auditorías deberán identificar riesgos potenciales y establecer medidas correctivas inmediatas, asegurando un control riguroso sobre el manejo de información crítica.

CAPÍTULO X: Ámbito de Aplicación y Coordinación

Artículo 13°. Ámbito de Aplicación

La ley se aplica a las Infraestructuras Estratégicas y Críticas ubicadas en el territorio nacional, incluyendo las Islas Malvinas, las Georgias del Sur, las Sandwich del Sur, las Orcadas del Sur, el Sector Antártico Argentino, sus espacios marítimos circundantes(Ley N.º 23.775 y Decreto 905/1990) y el espacio ultraterrestre. Si bien las infraestructuras vinculadas a la Defensa y la Seguridad Nacional están comprendidas en el marco general de esta ley, su protección y regulación se rigen por normativas específicas que contemplan sus particularidades y requerimientos operativos propios. Estas disposiciones especiales aseguran que las necesidades estratégicas y de seguridad inherentes a estos sectores sean adecuadamente atendidas dentro de un marco normativo especializado.

Artículo 14°. Coordinación con Otros Organismos

El COFIEC coordinará con la Secretaría de Inteligencia y otros organismos de defensa y seguridad, y colaborará con entes reguladores y programas nacionales en sectores estratégicos.

CAPÍTULO XI: Disposiciones Generales

Artículo 15°. Financiamiento

Los recursos del COFIEC serán supervisados por la Auditoría General de la Nación (AGN), que auditará su uso en capacitación y protección tecnológica. Los fondos no se destinarán a sueldos permanentes, salvo para contrataciones temporales de personal especializado.

Artículo 16°. Derogaciones

Deróguense la Resolución Ministerial de la Jefatura de Gabinete de Ministros 1523/2019, la Decisión Administrativa 641/2021 y todas las disposiciones que se opongan a la presente Ley.

Artículo 17°. Vigencia

La presente ley entrará en vigor a partir de su publicación en el Boletín Oficial.

Artículo 18°. De forma.

Lic. Marcela Pagano
Diputada de la Nación

ANEXO I

Procedimientos de Seguridad y Plazos de Implementación

El COFIEC desarrollará un conjunto de protocolos de seguridad aplicables a todas las infraestructuras estratégicas y críticas del país. Estos protocolos serán revisados y actualizados periódicamente para responder a nuevas amenazas y tecnologías emergentes. Las medidas de seguridad deberán implementarse dentro de los 180 días posteriores a la sanción de esta ley.

ANEXO II

Sectores Estratégicos y Críticos

Introducción: Los sectores estratégicos y críticos son aquellos cuya continuidad operativa y control son pilares para la seguridad nacional y el desarrollo económico de Argentina, incluyendo el ***conocimiento*** necesario para su sostenimiento. La disrupción de estas infraestructuras podría afectar tanto la soberanía nacional como la estabilidad económica y social del país. A continuación, se definen los sectores y áreas cuya protección es prioritaria.

1. **Energía y Recursos Naturales**: Infraestructuras relacionadas con la generación, transmisión y distribución de energía, así como la extracción de recursos naturales, fundamentales para el funcionamiento del país.

    i. **Generación de Energía**: Centrales nucleares, hidroeléctricas, térmicas, eólicas, solares y otras fuentes de energía. Se aplicarán medidas de seguridad física y cibernética, junto con auditorías periódicas para garantizar su integridad y operatividad.

    ii. **Transmisión y Distribución de Electricidad**: Redes de transmisión de alta y media tensión, subestaciones y líneas de distribución, cuya protección es esencial para evitar interrupciones masivas.

iii. **Producción y Distribución de Gas y Petróleo**: Yacimientos, refinerías, oleoductos, gasoductos y redes de distribución. Se incluirán monitoreo continuo y simulacros de emergencia para asegurar el suministro energético.

iv. **Minería**: Explotaciones de minerales estratégicos y metales preciosos, sujetos a auditorías periódicas para proteger su operatividad y resguardar estos recursos frente a amenazas.

2. **Transporte**: Infraestructuras esenciales para la movilidad y el comercio, cuya protección garantiza la operatividad del Estado y la conectividad nacional e internacional.

   i. **Transporte Terrestre**: Redes viales, ferroviarias y de transporte público, incluyendo puentes, túneles, estaciones y terminales, cuya interrupción afectaría la economía y movilidad de la población.

   ii. **Transporte Aéreo**: Aeropuertos, estaciones de radar y sistemas de control de tráfico aéreo, que contarán con controles de acceso, medidas de ciberseguridad y planes de contingencia.

   iii. **Transporte Marítimo y Fluvial**: Puertos, canales y terminales que garantizan el comercio y abastecimiento. Se implementarán medidas de vigilancia, control y planes de emergencia.

3. **Telecomunicaciones y Tecnologías de la Información**: Infraestructuras esenciales para las comunicaciones y la economía digital, cuya protección es crítica para la seguridad nacional.

   i. **Redes de Comunicación**: Torres de transmisión, sistemas de comunicación satelital, radio y televisión, vitales para la respuesta ante emergencias y el funcionamiento del Estado.

ii. **Servicios de Internet**: Proveedores de servicios de internet y centros de datos, que contarán con medidas avanzadas de ciberseguridad para prevenir ataques.

iii. **Sistemas de Información Críticos**: Infraestructuras que soportan bases de datos estatales y redes de información sensibles. Se establecerán planes de contingencia para garantizar su continuidad.

iv. **Soberanía Digital y Gestión Transfronteriza de Información Crítica para la Seguridad y Operación del Estado Nacional:** El **Estado Nacional** deberá garantizar la **soberanía digital**, asegurando que el almacenamiento y procesamiento primario de la **información crítica** se realice en "**data centers nacionales"**, bajo regulaciones que garanticen su **integridad, disponibilidad y seguridad**, evitando accesos no autorizados o manipulación por actores extranjeros. Se permitirá una **redundancia secundaria en infraestructura externa**, siempre que se cumplan estrictamente las normas de **protección de datos** y se garantice la **equivalencia en los niveles de seguridad**. La normativa deberá contemplar **criterios de compatibilidad operativa**, asegurando que las exigencias de gestión y resguardo de información crítica **se ajusten a la evolución tecnológica**, equilibrando la **protección, eficiencia y seguridad** dentro de un marco regulatorio que **fortalezca la autonomía digital y la seguridad del Estado Nacional**.

4. **Agua y Saneamiento**: Infraestructuras para la captación, tratamiento y distribución de agua potable y la gestión de aguas residuales, vitales para la salud pública.

   i. **Captación, Tratamiento y Distribución de Agua Potable**:Plantas de tratamiento y redes de distribución esenciales para el bienestar de la población.

   ii. **Gestión de Aguas Residuales**: Plantas de tratamiento y sistemas de alcantarillado, fundamentales para la salud pública y protección ambiental.

5. **Salud**: Infraestructuras Estratégicas y Críticas para la seguridad pública que aseguran la atención médica continua en situaciones de crisis.

    i. **Infraestructuras Hospitalarias y de Atención Médica**: Hospitales, centros de atención primaria y clínicas, indispensables para responder a emergencias sanitarias.

    ii. **Producción y Distribución de Medicamentos**: Fábricas, laboratorios y centros de distribución, sujetos a estrictos controles de seguridad para asegurar el suministro.

6. **Finanzas**: Infraestructuras esenciales para la estabilidad económica y el funcionamiento del sistema financiero.

    i. **Sistemas Bancarios**: Centros de datos bancarios y sistemas de respaldo, que aseguran la continuidad de las operaciones financieras.

    ii. **Mercados Financieros**: Sistemas que soportan operaciones bursátiles y otros mercados, protegidos contra interrupciones que afecten la economía.

    iii. **Sistemas de Pago**: Plataformas de transacciones electrónicas y redes de pago, esenciales para el comercio y la economía.

7. **Alimentación**: Infraestructuras que garantizan la seguridad alimentaria y deben ser protegidas para prevenir el desabastecimiento.

    i. **Producción de Alimentos**: Campos de cultivo, fábricas y centros de distribución necesarios para el suministro de alimentos.

    ii. **Procesamiento y Distribución de Alimentos**: Plantas de procesamiento y redes logísticas esenciales para la distribución de alimentos en todo el país.

8. **Espacio Ultraterrestre y Antártico**: Infraestructuras estratégicas en el espacio ultraterrestre y el territorio antártico, esenciales para la seguridad y soberanía.

    i. **Instalaciones Espaciales**: Satélites de comunicación, sistemas de navegación y estaciones de monitoreo espacial.

ii. **Instalaciones en el Territorio Antártico**: Bases científicas y sistemas logísticos en la Antártida.

9. **Protección de la Frontera Seca y Zonas Marítimas Soberanas**: La protección de la frontera y del territorio marítimo hasta las 200 millas es fundamental para la defensa de la soberanía territorial.

   i. **Frontera Seca**: Sistemas de monitoreo y vigilancia para proteger la integridad de las fronteras terrestres.

   ii. **Zonas Marítimas**: Sistemas de control en el territorio marítimo hasta las 200 millas y más allá, incluyendo el talud continental, para resguardar los recursos submarinos.

10. **Fauna Ictícola y Recursos Marítimos**: La protección de recursos marítimos y fauna ictícola es fundamental para la seguridad y economía, vigilados continuamente contra incursiones ilegales.

11. **Edificios de Valor Histórico y Cultural**: Estructuras cuya conservación es esencial por su relevancia histórica, arquitectónica, cultural, económica o social.

Lic. Marcela Pagano
Diputada de la Nación

FUNDAMENTOS

Señor Presidente:

El presente Proyecto de Ley tiene como objetivo la creación del Consejo Federal de Infraestructuras Estratégicas y Críticas (COFIEC), un organismo con la competencia de identificar, evaluar y proteger aquellas infraestructuras esenciales para la seguridad, soberanía y desarrollo económico de la Argentina. El COFIEC emitirá dictámenes vinculantes en procesos de privatización para asegurar que las infraestructuras estratégicas permanezcan bajo control nacional, evitando que intereses comerciales o externos comprometan la seguridad del país.

Según Aureliano Da Ponte[1], en el contexto actual, la tecnología ha emergido como un eje fundamental de poder e influencia, donde la pérdida de control sobre Infraestructuras Estratégicas y Críticas puede traducirse en desventajas estratégicas irreversibles para una nación.La geopolítica ha retomado una posición central en las decisiones de los responsables políticos, convirtiéndose en una variable crucial en múltiples áreas. Esto abarca desde las infraestructuras digitales críticas, como las comunicaciones avanzadas 5G y los cables submarinos, hasta el control de materias primas como las tierras raras, y sectores industriales estratégicos como la inteligencia artificial y los semiconductores. Además, cobra relevancia la regulación de los flujos de datos, su almacenamiento y la definición de estándares para las tecnologías emergentes. (Da Ponte, A., 2023, p. 3)

Esta perspectiva refuerza la misión del COFIEC de proteger las infraestructuras esenciales, preservando así la estabilidad y la independencia nacional de Argentina frente a factores de presión externos. Da Ponte subraya que la tecnología no solo transforma economías, sino que también es una fuerza que redistribuye el poder a

[1]Da Ponte, A. (2023) "Poder de Innovación e Inteligencia Artificial". CEPIUBA. Área de Inteligencia Artificial, N° 1, Diciembre.

nivel global, y para un país como Argentina, es vital mantener el control de estos activos estratégicos.

El COFIEC coordinará con organismos nacionales e internacionales, impulsará programas de capacitación y auditoría, y preservará capacidades industriales y científicas esenciales para la autosuficiencia nacional. La protección de infraestructuras estratégicas en sectores como energía, transporte, telecomunicaciones y recursos naturales es prioritaria, siguiendo prácticas de países como Estados Unidos (NationalInfrastructureProtection Plan, NIPP), Alemania, Francia, China e Israel, que han implementado legislaciones avanzadas para proteger sus activos estratégicos.

Soberanía Tecnológica y Autonomía Nacional

La soberanía tecnológica constituye uno de los pilares fundamentales para asegurar la autonomía y seguridad de los Estados en el contexto global. Según Da Ponte (2024)[2], la soberanía tecnológica implica la capacidad de una nación para desarrollar y mantener el control sobre tecnologías críticas, garantizando así su independencia en sectores clave y reduciendo vulnerabilidades frente a actores externos (Da Ponte, 2024., p.418). En línea con esta idea, el COFIEC desempeñará un rol crucial en la protección de las Infraestructuras Estratégicas y Críticas de Argentina, reforzando su resiliencia y capacidad de acción autónoma.

Importancia y Marco Contextual Actual

La Resolución Ministerial de la Jefatura de Gabinete de Ministros 1523/2019 y la Decisión Administrativa 641/2021 resultan insuficientes para una protección integral de las infraestructuras estratégicas, pues carecen de mecanismos de supervisión directa sobre sectores industriales y tecnológicos claves. En un contexto donde aumentan las amenazas a estos sectores fundamentales de nuestro quehacer nacional, la legislación actual no dispone de medidas específicas para garantizar la preservación

[2] Da Ponte, A. (2024). "Inteligencia Artificial en la carrera por el Siglo XXI. ¿Una tecnología dual que cambia las reglas del juego? (pp. 407-436). "La política Internacional en el Proceso de Transición Intersistémico. ¿Nuevas realidades? ¿Nuevos enfoques?". Salimena, G. Compilador. TESEOPRESS Publisher.

de estos activos esenciales. En contraste, países como Estados Unidos, Francia y otros, han adoptado políticas que regulan la privatización y adquisición de infraestructuras estratégicas para mantener su integridad y seguridad.

El Decreto 1107/2024, que intenta establecer y definir qué se entiende como "Objetivos de Valor Estratégico" y cuál debe ser su tratamiento, ha suscitado una considerable controversia en nuestro país, debido a sus implicancias legales, institucionales y democráticas. Haciendo un análisis exhaustivo,se exponen las razones por las cuales se solicita su derogación.

i. Ambigüedad en la definición de "Objetivos de Valor Estratégico"

Define estos objetivos como "cualquier bien, instalación o conjunto de instalaciones fijas y las entidades materiales de vital importancia para el Estado Nacional" cuya afectación podría ocasionar "graves perjuicios" a diversos aspectos del país. Esta definición es amplia y vaga, lo que permite una interpretación discrecional por parte del Poder Ejecutivo. Tal ambigüedad podría incluir desde Infraestructuras Estratégicas y Críticas hasta espacios públicos donde se desarrollan manifestaciones sociales, sindicales o políticas, habilitando la intervención de las Fuerzas Armadas en contextos de protesta.

ii. Concentración de poder en el Poder Ejecutivo

Otorga al Poder Ejecutivo Nacional la competencia exclusiva para calificar qué constituye un "Objetivo de Valor Estratégico", sin establecer mecanismos de control institucional ni participación del Congreso. Esta concentración de poder en el Ejecutivo, sin la intervención de organismos especializados o del poder legislativo, abre la puerta a decisiones arbitrarias y potencialmente autoritarias.

iii. Ampliación del rol de las Fuerzas Armadas en la seguridad interior

Permite la intervención de las Fuerzas Armadas en la protección de estos objetivos estratégicos, incluso en tiempos de paz y en situaciones de conmoción interior. Esto contraviene la Ley de Defensa Nacional Nº 23.554 y la Ley de Seguridad

Interior Nº 24.059, que establecen una clara separación entre las funciones de defensa nacional y seguridad interior. La participación de las Fuerzas Armadas en asuntos de seguridad interna sin una adecuada regulación y control legislativo representa un grave retroceso en materia de derechos ciudadanos, en el marco protestas sociales y conlleva a la criminalización de la disidencia.

iv. Posibles implicancias para el ejercicio de derechos civiles

La ambigüedad en la definición de "Objetivos de Valor Estratégico" permite que el Gobierno pueda considerar como tales a espacios públicos o instituciones donde se desarrollan manifestaciones sociales, sindicales o políticas. Esto habilita la intervención de las Fuerzas Armadas en contextos de protesta, lo cual es incompatible con un sistema democrático y con el respeto a los derechos fundamentales de reunión y expresión.

v. Precedente institucional y necesidad de revisión normativa por parte del Congreso de la Nación

La implementación de este Decreto sienta un precedente inquietante al permitir que el Poder Ejecutivo concentre facultades discrecionales para definir amenazas y desplegar fuerzas militares en el ámbito interno. Esto podría erosionar los controles institucionales y debilitar la protección de los derechos civiles y políticos. La historia argentina ha demostrado los peligros de involucrar a las Fuerzas Armadas en tareas internas, y este Decreto podría abrir la puerta a la repetición de episodios oscuros del pasado.

El Decreto 1107/2024 representa una medida que pone en riesgo los principios fundamentales del sistema democrático argentino. Su ambigüedad, concentración de poder en el Ejecutivo, ampliación del rol de las Fuerzas Armadas en la seguridad interior y falta de control institucional justifican su revisión o derogación. Es imperativo que se restablezca el respeto por la división de poderes, se garantice la participación del Congreso en decisiones de esta magnitud y se protejan los derechos y libertades fundamentales de todos los ciudadanos.

Marco normativo de ciberseguridad

La Ley de Delitos Informáticos N° 26.388, la Ley de Protección de Datos Personales N° 25.326, y la Ley de Firma Digital N° 25.506 reflejan un marco de protección de ciberseguridad limitado en alcance. Este proyecto de ley, al integrar aspectos de ciberseguridad en la gestión de Infraestructuras Estratégicas y Críticas, responde a la necesidad de una normativa integral que proteja activos sensibles en todos los sectores.

Tecnología como bien estratégico

El conocimiento aplicado en Infraestructuras Estratégicas y Críticas debe ser considerado un bien estratégico. Sectores de alta tecnología, como la energía nuclear y la aviación, dependen de competencias acumuladas a lo largo de décadas, las cuales resultan difíciles de recuperar una vez perdidas. Esta perspectiva se alinea con el análisis deLoizou, N. (2022, pp. 93-114)[3], quien destaca la importancia de desarrollar y proteger capacidades nacionales de ciencia y tecnología aplicadas a la defensa. Asimismo, subraya que el conocimiento y la tecnología en contextos críticos poseen un valor estratégico cuya pérdida puede amenazar tanto la soberanía como la capacidad operativa del país.

De manera complementaria, Da Ponte (2023, pp. 8-9) sostiene que las capacidades tecnológicas estratégicas permiten a los Estados mantener una ventaja competitiva, no solo en términos económicos, sino también en el ámbito geopolítico.

Así, el COFIEC, en su misión de preservar y proteger las Infraestructuras Estratégicas y Críticas, deberá considerar estos principios para reforzar la autonomía nacional y asegurar la seguridad a largo plazo.

Iniciativas nacionales de ciberseguridad

---

[3] Loizou, N. (2022). "La política científico-tecnológica de la Defensa en Argentina: Desarrollo institucional durante la primera etapa del desarrollismo inclusivo semiperiférico (2003-2007)". Revista **Ucronías**, N° 6.Centro de Estudios de Historia de la Ciencia y la Técnica "José Babini" (Escuela de Humanidades, UNSAM), Argentina

Argentina ha avanzado en ciberseguridad con programas como el Programa Nacional de Protección de Infraestructuras Estratégicas y Críticas de Información y Ciberseguridad, y la creación del Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar). Sin embargo, queda pendiente una visión estratégica más integral que permita una protección y respuesta adecuadas para sectores críticos.

Conservación de capacidades tecnológicas nacionales

Las capacidades tecnológicas de Argentina, desarrolladas a lo largo de décadas, pueden desaparecer rápidamente si no se protegen. Empresas en sectores como el nuclear y energético son consideradas patrimonio estratégico del Estado, y el COFIEC debe asegurar su preservación frente a privatizaciones que comprometan este conocimiento acumulado.

La importancia de proteger las infraestructuras estratégicas

Las infraestructuras estratégicas, como las redes de energía, transporte, telecomunicaciones y recursos naturales son esenciales para el desarrollo económico y la seguridad nacional. La disrupción de estos sistemas comprometería no solo la defensa nacional, sino también la estabilidad económica y social del país. En Estados Unidos, la "CriticalInfrastructureProtectionAct" (CIPA) es una ley clave que protege infraestructuras vulnerables frente a ciberamenazas y otros ataques. Francia prioriza la defensa de sus instalaciones nucleares como parte de su política de seguridad energética y nacional. Este Proyecto de Ley busca adoptar y adaptar estos modelos de protección a la realidad argentina.

El rol del COFIEC como garante de la soberanía nacional

Este Proyecto de Ley establece al COFIEC como un organismo con capacidad de emitir dictámenes vinculantes en privatizaciones de empresas estratégicas, asegurando que el control de sectores clave permanezca en manos nacionales. Alemania, por ejemplo, limita la adquisición de empresas estratégicas por capitales extranjeros, subrayando la importancia de un regulador que proteja la soberanía. El

COFIEC supervisará y regulará decisiones de privatización en Argentina, protegiendo sectores sensibles y la independencia económica.

Evaluación exhaustiva en privatización de empresas estratégicas

El Proyecto de Ley exige que cualquier intento de privatización de empresas estatales estratégicas sea evaluado exhaustivamente por el COFIEC. Este proceso incluye la emisión de un informe detallado y un dictamen vinculante, siguiendo prácticas internacionales como las de la OTAN, China y Corea del Sur, donde se aplican estrictos controles para la privatización de activos estratégicos. El COFIEC garantizará que estas decisiones se basen en un análisis profundo de las implicancias en seguridad y desarrollo nacional.

Infraestructuras Estratégicas y Críticas como pilares de la seguridad nacional

Las Infraestructuras Estratégicas y Críticas son componentes esenciales para la estabilidad de un país. El NationalInfrastructureProtection Plan (NIPP) en Estados Unidos destaca que estas infraestructuras son vitales para la seguridad nacional. Siguiendo esta lógica, el COFIEC se establece como el organismo principal para identificar y proteger infraestructuras estratégicas y críticas en Argentina, asegurando salvaguardas adecuadas en defensa de los intereses nacionales.

Lecciones de políticas comparadas sobre privatización y soberanía

En países como Reino Unido, la "National Security and InvestmentAct" permite bloquear adquisiciones que comprometan la seguridad nacional. China reserva el control mayoritario en sectores críticos exclusivamente al Estado, y Alemania restringe la adquisición de empresas estratégicas. Este Proyecto de Ley establece un mecanismo similar de revisión para garantizar que cualquier intento de privatización en Argentina esté acompañado de un análisis de impacto sobre la soberanía y desarrollo nacional.

Capacitación y formación como pilares de la resiliencia tecnológica

El Proyecto de Ley requiere que las empresas que gestionen Infraestructuras Estratégicas y Críticas destinen parte de su presupuesto a capacitación y auditoría, fortaleciendo la resiliencia tecnológica y una cultura de seguridad operativa. Esto asegura que el personal esté capacitado para responder ante emergencias y proteja tanto la seguridad física como la cibernética.

El Proyecto de Ley que crea el "Consejo Federal de Infraestructuras Estratégicas y Críticas - (COFIEC)" responde a la necesidad de proteger los activos esenciales de Argentina, preservar sus capacidades tecnológicas y garantizar la soberanía nacional. Inspirada en las mejores prácticas internacionales, esta Ley establece los mecanismos necesarios para que las decisiones sobre privatización y control de Infraestructuras Estratégicas y Críticas se basen en un análisis cuidadoso y profundo. Al asegurar que los sectores estratégicos permanezcan bajo control nacional, Argentina construye una defensa integral de sus activos más importantes, garantizando estabilidad, seguridad y desarrollo.

Lic. Marcela Pagano
Diputada de la Nación