

**ARGENTINA**  
**HONORABLE CONGRESO DE LA NACIÓN**

**MARCO INTEGRAL PARA LA SOBERANÍA  
DIGITAL,  
LA TRANSPARENCIA ECONÓMICA  
Y LA TRANSICIÓN TECNOLÓGICA  
SOSTENIBLE**

Paquete de Leyes Estratégicas para la Gobernanza de Datos,  
la Inversión Responsable, la Seguridad Digital  
y el Desarrollo Tecnológico Inclusivo

Autora: Natividad Vidal  
Capilla del Monte, Córdoba – República Argentina  
Año 2025

# PRÓLOGO

## **Marco Integral para la Soberanía Digital, la Transparencia Económica y la Transición Tecnológica Sostenible**

La República Argentina atraviesa una transformación profunda impulsada por la digitalización de la economía, la automatización de procesos productivos, la expansión de los datos como activo estratégico y el avance acelerado de tecnologías emergentes como la inteligencia artificial.

Este proceso, global e irreversible, presenta oportunidades inéditas para el desarrollo, la eficiencia y la innovación, pero también riesgos sistémicos asociados a la concentración de poder económico, la opacidad financiera, la fragmentación institucional, la vulnerabilidad cibernética y la exclusión social derivada de transiciones tecnológicas no planificadas.

El presente **Marco Integral para la Soberanía Digital, la Transparencia Económica y la Transición Tecnológica Sostenible** surge como respuesta estructural del Estado argentino a estos desafíos, con el objetivo de establecer reglas claras, previsibles y modernas que permitan gobernar la tecnología, los datos y los flujos económicos estratégicos en beneficio del interés público y del desarrollo nacional.

El paquete legislativo que integra este Marco reconoce a los **datos, la infraestructura digital, la ciberseguridad, la energía, el conocimiento y los activos económicos estratégicos** como componentes centrales de la soberanía contemporánea. En este sentido, se propone fortalecer la capacidad del Estado para garantizar transparencia, trazabilidad, seguridad jurídica, equidad distributiva y sostenibilidad ambiental, sin obstaculizar la innovación ni la inversión responsable.

Las leyes que componen este Marco han sido diseñadas de manera **autónoma pero armónica**, respetando la división de competencias, la seguridad jurídica y los estándares internacionales vigentes, al tiempo que incorporan mecanismos de cooperación interinstitucional, federalismo operativo y control ciudadano.

Este enfoque integral permite abordar de forma coordinada aspectos clave como:

- la apertura y gobernanza soberana de los datos públicos,
- la tokenización ética y trazable de activos,
- la transparencia de beneficiarios reales,
- la declaración y supervisión de activos estratégicos externos,
- la promoción de inversiones con contrapartidas reales,
- la distribución social de la renta tecnológica,
- la sostenibilidad ambiental de la infraestructura digital,
- y la protección de la identidad y la seguridad digital de las personas.

El Marco no persigue fines punitivos ni restrictivos, sino **ordenadores y preventivos**, orientados a reducir riesgos macroeconómicos, fortalecer la confianza institucional, mejorar el clima de inversión y asegurar que el desarrollo tecnológico contribuya efectivamente al bienestar social y al desarrollo sostenible.

En un contexto internacional marcado por tensiones geopolíticas, reconfiguración de cadenas de valor y creciente regulación tecnológica, la Argentina se propone, a través de este Marco, posicionar como una **jurisdicción confiable, transparente y preparada**, capaz de integrar innovación, derechos, sostenibilidad y estabilidad institucional.

Este conjunto de leyes expresa una visión de largo plazo, orientada a consolidar una **arquitectura legal de Estado**, que trascienda coyunturas políticas y contribuya a construir un futuro digital soberano, inclusivo y sustentable para la Nación.

# **RESUMEN EJECUTIVO UNIFICADO**

## **PAQUETE DE LEYES PARA LA SOBERANÍA DIGITAL, TRANSPARENCIA ECONÓMICA Y TRANSICIÓN TECNOLÓGICA SOSTENIBLE**

**Argentina**

---

### **1. Visión general del paquete normativo**

El presente paquete de **ocho leyes articuladas** constituye una **arquitectura jurídica integral** destinada a ordenar la transformación digital, económica y social de la República Argentina bajo principios de:

- soberanía de datos y activos estratégicos,
- transparencia y trazabilidad económica,
- atracción de inversiones con reglas claras,
- sostenibilidad ambiental y tecnológica,
- protección de derechos digitales,
- cohesión social frente a la automatización.

No se trata de normas aisladas, sino de un **sistema coherente**, diseñado para reducir riesgos estructurales, mejorar la previsibilidad macroeconómica y acompañar el desarrollo tecnológico con responsabilidad institucional.

---

### **2. Problema estructural que aborda el paquete**

La economía digital y la globalización financiera han generado:

- fragmentación normativa,
- opacidad patrimonial,
- fuga de rentas estratégicas,
- presión sobre recursos naturales y energéticos,

- vulnerabilidad cibernética,
- desplazamientos laborales por automatización.

Sin un marco integral, estos procesos **debilitan la soberanía, la estabilidad y la legitimidad social del desarrollo tecnológico**.

Este paquete propone una **respuesta sistemática**, moderna y alineada con estándares internacionales.

---

### **3. Ley madre: Datos Abiertos Soberanos**

La **Ley de Datos Abiertos Soberanos** es el eje estructurante del sistema. Establece que los datos públicos y estratégicos deben ser:

- abiertos, interoperables y trazables,
- auditables por el Estado y la ciudadanía,
- protegidos frente a usos indebidos,
- considerados infraestructura estratégica.

Todas las demás leyes **se apoyan en esta base común de información confiable**.

---

### **4. Tokenización Ética y trazabilidad digital**

La **Ley de Tokenización Ética** introduce herramientas digitales para:

- registrar activos, derechos y flujos,
- garantizar trazabilidad y auditabilidad,
- evitar manipulación o apropiación indebida.

La tokenización se concibe como **instrumento de confianza pública**, no como especulación financiera.

---

### **5. Transparencia y Beneficiarios Reales**

La **Ley de Transparencia y Registro de Beneficiarios Reales** establece la identificación obligatoria de las personas humanas que controlan o se benefician de estructuras jurídicas.

Es condición habilitante para:

- contratar con el Estado,
- acceder a subsidios o regímenes promocionales,
- participar del RIGI.

La transparencia se define como **requisito de previsibilidad**, no como sanción.

---

## 6. Declaración Obligatoria de Activos Estratégicos Externos

Esta ley permite conocer:

- quién controla activos estratégicos,
- dónde se encuentran,
- cómo impactan en la economía nacional.

Se articula con beneficiarios reales y datos abiertos para **prevenir fuga estructural de capitales**, fortalecer reservas y proteger la estabilidad macroeconómica.

---

## 7. Ampliación del RIGI y Renta Tecnológica Social

La **Ampliación del RIGI** redefine los incentivos a grandes inversiones, incorporando:

- transparencia patrimonial,
- sostenibilidad ambiental y tecnológica,
- transferencia de conocimiento,
- desarrollo federal.

Se crea el **FONARETS**, que transforma parte de la renta tecnológica y extraordinaria en:

- inversión social,
- formación digital,
- infraestructura tecnológica pública.

Esto fortalece el RIGI, evitando abusos y mejorando su legitimidad.

---

## 8. Renta Básica Tecnológica y Transición Digital

La **Ley de Renta Básica Tecnológica** es una política de transición, no asistencial.

Acompaña a personas afectadas por:

- automatización,
- digitalización intensiva,
- cambios productivos estructurales.

Se implementa de manera:

- gradual,
- fiscalmente sostenible,
- articulada con empleo y formación.

Se financia prioritariamente con renta tecnológica, no con endeudamiento.

---

## **9. Sostenibilidad Ambiental Tecnológica**

Esta ley asegura que el desarrollo digital y la IA:

- no comprometan recursos hídricos y energéticos,
- utilicen energías renovables,
- incorporen eficiencia y economía circular,
- evalúen impactos acumulativos.

Incluye reglas claras para **centros de datos, infraestructuras de IA y plataformas tecnológicas**, evitando conflictos socioambientales futuros.

---

## **10. Ciberseguridad e Identidad Digital**

La **Ley de Ciberseguridad e Identidad Digital** protege:

- infraestructuras críticas,
- sistemas económicos y financieros,
- identidad de las personas,
- derechos digitales.

Establece estándares, protocolos de respuesta y gobernanza institucional, alineados con ISO, NIST, OCDE y ONU.

La ciberseguridad se reconoce como **infraestructura estratégica del desarrollo**.

---

## **11. Coherencia y articulación del sistema**

Las ocho leyes:

- comparten principios comunes,
- evitan superposiciones,
- se refuerzan mutuamente,
- reducen discrecionalidad,
- aumentan previsibilidad jurídica.

El paquete forma una **arquitectura de Estado**, no una política coyuntural.

---

## **12. Impacto esperado**

- mejora estructural del clima de inversión,
  - reducción de riesgos macroeconómicos,
  - fortalecimiento de soberanía digital y económica,
  - desarrollo tecnológico sostenible,
  - mayor cohesión social en la transición digital,
  - alineación con estándares internacionales.
- 

## **13. Conclusión**

Este paquete de leyes **no frena el desarrollo**.

Lo **ordena, transparenta y vuelve sostenible**.

Propone un modelo donde:

- la innovación genera confianza,
- la inversión tiene reglas claras,
- la tecnología beneficia a toda la sociedad,
- el Estado recupera capacidad estratégica.

Es una **propuesta de país para la era digital**.

# ÍNDICE GENERAL

## Marco Integral para la Soberanía Digital, la Transparencia Económica y la Transición Tecnológica Sostenible

---

### DOCUMENTOS INTRODUCTORIOS

- Portada Institucional
  - Prólogo
  - Resumen Ejecutivo Unificado
- 

### CUERPO NORMATIVO

#### Paquete de Leyes Estratégicas

---

##### I. Ley de Datos Abiertos Soberanos

(*Ley Marco del Sistema Nacional de Datos Soberanos Abiertos*)

- Objeto y principios
  - Alcance y definiciones
  - Gobernanza de datos públicos
  - Interoperabilidad y estándares
  - Control ciudadano y auditoría
  - Anexos técnicos
- 

##### II. Ley de Tokenización Ética y Trazabilidad Digital

- Marco conceptual y definiciones
- Principios éticos de tokenización
- Registro, trazabilidad y auditoría
- Integración con datos abiertos

- Protección de derechos
  - Anexos técnicos
- 

### **III. Ley de Transparencia y Registro de Beneficiarios Reales**

- Objeto y sujetos obligados
  - Beneficiario real y control efectivo
  - Registro público y acceso a la información
  - Integración con sistemas nacionales
  - Sanciones y fiscalización
  - Anexos operativos
- 

### **IV. Ley de Declaración Obligatoria de Activos Estratégicos Externos**

- Definición de activos estratégicos
  - Sujetos obligados
  - Régimen de declaración y auditoría
  - Repatriación y reinversión
  - Cooperación internacional
  - Régimen sancionatorio
  - Anexos de implementación
- 

### **V. Ley de Ampliación del RIGI y Renta Tecnológica Social (FONARETS)**

- Objetivos y alcance
  - Ampliación del régimen de incentivos
  - Contrapartidas productivas y tecnológicas
  - Fondo Nacional de Renta Tecnológica
  - Transparencia y control
  - Anexos financieros y operativos
-

## **VI. Ley de Renta Básica Tecnológica y Transición Digital Sostenible**

- Fundamentos y objetivos
  - Fuente de financiamiento
  - Mecanismos de asignación
  - Transición laboral y social
  - Evaluación de impacto
  - Anexos de implementación
- 

## **VII. Ley de Sostenibilidad Ambiental Tecnológica**

- Principios ambientales aplicados a tecnología
  - Centros de datos e infraestructura digital
  - Energía, agua y eficiencia
  - Evaluación de impacto ambiental
  - Anexo especial de Data Centers
  - Anexos técnicos complementarios
- 

## **VIII. Ley de Ciberseguridad e Identidad Digital**

- Infraestructura crítica digital
  - Identidad digital y protección de datos
  - Gestión de riesgos cibernéticos
  - Protocolos de incidentes
  - Certificación y auditoría
  - Anexos técnicos y operativos
- 

## **DOCUMENTOS DE CIERRE**

- Cláusula de Articulación y Complementariedad Normativa
- Disposiciones finales

# **PROYECTO DE LEY**

## **Ley de Datos Abiertos, Éticos y Soberanos de Argentina**

### **– 2025**

#### **Autora:**

Natividad Vidal

Capilla del Monte, Córdoba, Argentina

**Correo Institucional:** [datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

#### **Presentado ante:**

Honorable Cámara de Diputados de la Nación

Honorable Cámara de Senadores de la Nación

**Fecha:** \_\_\_\_\_



Natividad Vidal  
DNI 27.716.481

Proyecto presentado para su tratamiento en el marco del Programa de Soberanía Digital Argentina, alineado con estándares ONU – CEPAL – OGP.

## **INDICE GENERAL**

### **PARTE I — TEXTO DEL PROYECTO DE LEY**

- **TÍTULO I — DISPOSICIONES GENERALES**
- **TÍTULO II — GOBERNANZA NACIONAL DE DATOS SOBERANOS: CREACION DE LA ANDAS Y DEL PORTAL NACIONAL DE DATOS ABIERTOS Y SOBERANOS.**
- **TÍTULO III — REGISTRO NACIONAL DE ACTIVOS Y BIENES ESTRATEGICOS DEL ESTADO (RNADE) GESTIÓN Y PROTECCIÓN DE DATOS PERSONALES POR EL ESTADO. LOS DERECHOS DIGITALES**
- **TÍTULO IV — PUBLICACIÓN OBLIGATORIA DE DATOS ABIERTOS, ETICA Y TRANSPARENCIA ALGORITMICA.**
- **TÍTULO V - INFORMACION CLASIFICADA POR SEGURIDAD NACIONAL**
- **TÍTULO VI — FINANCIAMIENTO Y SOSTENIBILIDAD PRESUPUESTARIA.**
- **TÍTULO VII - PREVENCIÓN DE CONCENTRACIÓN DIGITAL Y AUDITORÍA CIUDADANA DIGITAL (MACD)**
- **TÍTULO VIII — INTELIGENCIA ARTIFICIAL ETICA Y SOBERANA**
- **TÍTULO IX — PROTECCIÓN DE DATOS BIOMÉTRICOS Y SENSIBLES**
- **TÍTULO X — REGULACIÓN Y TRANSPARENCIA DEL ENTORNO DIGITAL DOMÉSTICO**
- **TÍTULO XI — ESTÁNDARES INTERNACIONALES**
- **TÍTULO XII — ARMONIZACIÓN NORMATIVA NACIONAL**
- **TÍTULO XIII — DISPOSICIONES SOBRE RIESGOS DIGITALES**
- **TÍTULO XIV — DERECHOS DIGITALES DEL USUARIO**
- **TÍTULO XV — TRANSPARENCIA EN INFRAESTRUCTURA DE RED**
- **TÍTULO XVI – INTEGRIDAD ALGORITMICA, AUDITORIA Y GOBERNANZA HUMANA DE DATOS**
- **TÍTULO XVII — TOKENIZACIÓN ÉTICA (RÉGIMEN GENERAL)**
- **TÍTULO XVIII — RESPONSABILIDAD Y PENALIDADES**
- **TÍTULO XIX — IMPLEMENTACIÓN Y FASES**
- **TÍTULO XX — COMPATIBILIDAD FISCAL**
- **TÍTULO XXI — DISPOSICIONES FINALES**
- **FUNDAMENTOS**

## **PARTE II — ANEXOS TÉCNICOS INTEGRADOS**

- **ANEXO I — PLAN ESTRATEGICO DE IMPLEMENTACION**
- **ANEXO II — EVALUACIÓN ECONÓMICA, FISCAL Y REDUCCIÓN DE CAPEX**
- **ANEXO III — INCENTIVOS PARA TECNOLÓGICAS E INVERSORES (NO FISCALES)**
- **ANEXO IV — INFORME TÉCNICO CIUDADANO SOBRE CGNAT Y ESTABILIDAD**
- **ANEXO V — MARCO INTERNACIONAL (CEPAL – ONU – OGP)**
- **ANEXO VI — METODOLOGÍA DE TOKENIZACIÓN ÉTICA**

## **PARTE III — ANEXOS COMPLEMENTARIOS**

- Matrices técnicas
- Cuadros comparados
- Glosario técnico
- Resumen Ejecutivo para Comisiones

# TÍTULO I — DISPOSICIONES GENERALES

## Artículo 1° — Objeto

La presente ley tiene por objeto establecer un régimen obligatorio de apertura, interoperabilidad, gobernanza ética y soberana de los datos públicos, garantizando su publicación en formatos abiertos, trazables y reutilizables, con el fin de fortalecer la transparencia, la participación ciudadana, la innovación pública y privada, y la soberanía digital de la Nación.

## Artículo 2° — Alcance

Las disposiciones de esta ley son de aplicación obligatoria para:

- a) La **Administración Pública Nacional** centralizada y descentralizada.
- b) **Activos internos y externos y Bienes Estratégicos** de la Nación.
- c) **Empresas y sociedades del Estado.**
- d) **Entes reguladores, organismos desconcentrados y agencias nacionales.**
- e) **Universidades nacionales** en todo procedimiento financiado con recursos públicos.
- f) **Proveedores contratistas** del Estado en aquello que se refiera a datos, sistemas y desarrollos financiados con fondos públicos.
- g) Toda institución que **reciba transferencias, subsidios o asistencia del Estado** y genere datos de relevancia pública.
- h) Todo **banco nacional o privado, institución financiera o entidad de intermediación de capital que administre fondos públicos**, recursos estratégicos, reservas, divisas o activos en el país o en el exterior.

## Artículo 3° – Bienes y Activos Estratégicos Sujetos a Datos Soberanos Abiertos

1. Se consideran **bienes y activos estratégicos de la Nación**, sujetos a publicación en **datos abiertos, trazabilidad y auditoría**, los siguientes:

### a) Recursos naturales y físicos estratégicos

1. Reservas de petróleo, gas, combustibles estratégicos y biocombustibles.
2. Centrales eléctricas, redes de transmisión y distribución energética.

3. Reservas y explotaciones de minerales estratégicos, incluyendo oro, plata, litio, cobre, uranio y tierras raras.
4. Embalses, ríos regulados, infraestructura de captación y distribución de agua potable e irrigación.
5. Bosques, áreas protegidas y biodiversidad con valor económico, estratégico o científico.
6. Suelo y tierras agrícolas estratégicas, incluyendo reservas de granos y semillas esenciales.

**b) Activos financieros y económicos estratégicos**

1. Reservas internacionales de oro, divisas, bonos soberanos y otros instrumentos financieros del Estado.
2. Activos financieros en el exterior, incluyendo inversiones, filiales internacionales, dividendos y utilidades de empresas estratégicas.
3. Fondos públicos estratégicos, incluyendo fondos de pensión y fondos destinados a infraestructura o desarrollo tecnológico.
4. Criptoactivos soberanos emitidos por el Estado o vinculados a la economía nacional.

**c) Empresas y sectores estratégicos**

1. Empresas con participación estatal directa o indirecta.
2. Empresas privadas que administren fondos públicos, subsidios, concesiones, licencias o bienes estratégicos.
3. Sectores estratégicos: energía, transporte, telecomunicaciones, agroindustria, salud, educación e infraestructura crítica.
4. Filiales, subsidiarias o participaciones internacionales de las empresas mencionadas.

**d) Infraestructura crítica**

1. Redes de transporte: puertos, aeropuertos, ferrocarriles estratégicos y vías de comunicación esenciales.
2. Redes de telecomunicaciones, internet, fibra óptica y satélites de comunicaciones.
3. Plantas de energía, plantas de tratamiento de agua y servicios esenciales.
4. Infraestructura de seguridad y defensa nacional.

**e) Bienes intangibles y tecnológicos**

1. Propiedad intelectual estratégica: patentes, software crítico y desarrollos tecnológicos de interés nacional.
2. Datos estratégicos: información geoespacial, censos, información de infraestructura crítica y bases de datos públicas.
3. Investigación y desarrollo financiado total o parcialmente con fondos públicos.

#### **f) Otros activos trazables y auditables**

1. Licencias, concesiones y permisos otorgados por el Estado.
2. Contratos de inversión y financiamiento público-privado.
3. Inventarios de bienes del Estado y equipamiento industrial, vehículos, aeronaves y embarcaciones estratégicas.
4. Todas las entidades que administren estos bienes y activos estarán obligadas a:
  - a) Publicar **información completa, abierta, auditabile y trazable** sobre la gestión, estado y destino de los mismos.
  - b) Garantizar **auditoría externa independiente** y accesible al público.
  - c) Reportar de forma periódica, según lo determine la autoridad competente, incluyendo activos nacionales y en el exterior.
  - d) Implementar mecanismos de control interno que aseguren la integridad, disponibilidad y trazabilidad de los datos.
5. El incumplimiento de estas obligaciones será sancionado conforme a lo previsto en esta Ley y en la normativa complementaria, incluyendo multas, auditorías forzadas y restricciones en el acceso a fondos, subsidios o concesiones estatales.

#### **g) Sistema financiero y activos externos estratégicos**

1. Se considera **activo estratégico de la Nación** a todo banco, institución financiera o entidad de intermediación de capital que administre fondos públicos, recursos estratégicos, reservas, divisas o activos en el país o en el exterior.
2. Todos los bancos e instituciones financieras **estatales** y todos los Bancos e instituciones financieras **privadas** que Administren fondos públicos o subsidios del Estado y Gestione activos estratégicos de la Nación, incluyendo divisas, reservas, bonos o inversiones vinculadas a sectores estratégicos o Mantengan activos externos de relevancia económica o estratégica para el país.
3. Estas entidades deberán:
  - a) Declarar obligatoriamente **todos los activos externos de su propiedad o bajo su administración**, incluyendo depósitos, inversiones, bonos, participaciones y filiales, indicando jurisdicción y tipo de activo.
  - b) Publicar la información en **formato abierto, auditabile y trazable**, integrando los datos al Registro Nacional de Activos Estratégicos Externos.
  - c) Someterse a **auditoría externa e independiente**, permitiendo la verificación de los activos estratégicos, tanto internos como externos.
4. Las obligaciones de declaración y transparencia se aplican también a **los activos estratégicos del sector privado** que administren fondos públicos o participen en sectores estratégicos definidos en la ley.
5. Publicar esta información en **formato abierto, auditabile y trazable**, integrándola al Registro Nacional de Activos Estratégicos.
  - c) Someterse a **auditoría externa independiente**, al igual que la banca estatal, permitiendo la verificación de activos internos y externos.
  - d) Facilitar información para la **repatriación de capitales estratégicos** según lo dispuesto en la Ley de Datos Soberanos Abiertos.

6. Sanciones por incumplimiento: Multas proporcionales al monto no declarado o a activos externos no repatriados, Suspensión de permisos, licencias o acceso a líneas de financiamiento público, Auditorías forzadas y publicación del incumplimiento en el registro público.

## **Artículo 4° — Bienes y Activos Estratégicos, Repatriación, Reversión Interna y Plazos**

1. Se consideran **bienes y activos estratégicos de la Nación**, sujetos a publicación en **datos abiertos, trazabilidad y auditoría**, los siguientes:

### **a) Recursos naturales y físicos estratégicos**

1. Reservas de petróleo, gas, combustibles estratégicos y biocombustibles.
2. Centrales eléctricas, redes de transmisión y distribución energética.
3. Reservas y explotaciones de minerales estratégicos, incluyendo oro, plata, litio, cobre, uranio y tierras raras.
4. Embalses, ríos regulados, infraestructura de captación y distribución de agua potable e irrigación.
5. Bosques, áreas protegidas y biodiversidad con valor económico, estratégico o científico.
6. Suelo y tierras agrícolas estratégicas, incluyendo reservas de granos y semillas esenciales.

### **b) Activos financieros y económicos estratégicos**

1. Reservas internacionales de oro, divisas, bonos soberanos y otros instrumentos financieros del Estado.
2. Activos financieros en el exterior, incluyendo inversiones, filiales internacionales, dividendos y utilidades de empresas estratégicas.
3. Fondos públicos estratégicos, incluyendo fondos de pensión y fondos destinados a infraestructura o desarrollo tecnológico.
4. Criptoactivos soberanos emitidos por el Estado o vinculados a la economía nacional.

### **c) Empresas y sectores estratégicos**

1. Empresas con participación estatal directa o indirecta.
2. Empresas privadas que administren fondos públicos, subsidios, concesiones, licencias o bienes estratégicos.
3. Sectores estratégicos: energía, transporte, telecomunicaciones, agroindustria, salud, educación e infraestructura crítica.
4. Filiales, subsidiarias o participaciones internacionales de las empresas mencionadas, incluyendo filiales en jurisdicciones consideradas paraísos fiscales.

### **d) Infraestructura crítica**

1. Redes de transporte: puertos, aeropuertos, ferrocarriles estratégicos y vías de comunicación esenciales.
2. Redes de telecomunicaciones, internet, fibra óptica y satélites de comunicaciones.
3. Plantas de energía, plantas de tratamiento de agua y servicios esenciales.
4. Infraestructura de seguridad y defensa nacional.

**e) Bienes intangibles y tecnológicos**

1. Propiedad intelectual estratégica: patentes, software crítico y desarrollos tecnológicos de interés nacional.
2. Datos estratégicos: información geoespacial, censos, información de infraestructura crítica y bases de datos públicas.
3. Investigación y desarrollo financiado total o parcialmente con fondos públicos.

**f) Otros activos trazables y auditables**

1. Licencias, concesiones y permisos otorgados por el Estado.
2. Contratos de inversión y financiamiento público-privado.
3. Inventarios de bienes del Estado y equipamiento industrial, vehículos, aeronaves y embarcaciones estratégicas.
4. Las entidades que administren estos bienes y activos deberán:
  - a) Publicar **información completa, abierta, auditabile y trazable** sobre la gestión, estado y destino de los mismos, incluyendo activos nacionales y en el exterior.
  - b) Repatriar **un mínimo del 50% de los dividendos y utilidades generadas en el exterior** para su reinversión en proyectos estratégicos dentro del país.
  - c) Liquidar al mercado local **al menos el 30% de las divisas repatriadas**, contribuyendo así al fortalecimiento de reservas internacionales.
  - d) Repatriación y liquidación deberán realizarse **en un plazo máximo de 180 días** desde la generación del ingreso o dividendos.
  - e) Incluir información sobre **filiales, subsidiarias y participaciones en jurisdicciones consideradas paraísos fiscales**, detallando flujos, activos y dividendos pendientes.
  - f) Garantizar **auditoría externa independiente** y accesible al público.
  - g) Reportar trimestralmente:
    - Montos repatriados y liquidados
    - Destino de la reinversión interna
    - Flujos de capital pendientes de repatriación
5. Sanciones por incumplimiento:
  - a) **Multas proporcionales** al monto de activos externos no repatriados o divisas no liquidadas, escalonadas según retraso:
    - 1–30 días: 10% del monto pendiente
    - 31–90 días: 25% del monto pendiente
    - 90 días: 50% del monto pendiente
  - b) Suspensión temporal de acceso a subsidios, concesiones, contratos públicos o financiamiento estatal.

- c) Auditorías forzadas y obligatorias por organismos de control competentes, con publicación inmediata de resultados.
- d) Bloqueo preventivo de nuevas filiales o operaciones externas hasta cumplir obligaciones de repatriación y liquidación.

## **Artículo 5° – Plan de repatriación obligatoria de activos estratégicos en paraísos fiscales y empresas fantasma**

### **1. Objeto**

Establecer un mecanismo obligatorio de **repatriación de capitales y activos estratégicos** ubicados en el exterior a través de **filiales, subsidiarias o empresas fantasma**, que se encuentren en jurisdicciones consideradas paraísos fiscales, con el objetivo de proteger la soberanía económica, incrementar reservas y prevenir fuga de capitales.

### **2. Sujetos obligados**

- Empresas con **participación estatal directa o indirecta**.
- Empresas privadas que administren **fondos públicos, subsidios, concesiones, licencias o bienes estratégicos**, y que tengan filiales, subsidiarias o participaciones en paraísos fiscales.
- Cualquier entidad vinculada con **activos estratégicos de la Nación** detectados en investigaciones previas de vaciamiento o remisión de capitales.

### **3. Inventario obligatorio**

- Todas las entidades deberán presentar un **inventario completo de activos y capitales externos** en jurisdicciones offshore o empresas fantasma, incluyendo:
  - Filiales, subsidiarias o participaciones indirectas.
  - Dividendos, utilidades retenidas y cualquier flujo financiero.
  - Activos tangibles o intangibles vinculados con proyectos estratégicos nacionales.

### **4. Plazos de repatriación**

- **Fase 1 – Inventario y declaración inicial:** 60 días desde la promulgación de la ley.
- **Fase 2 – Repatriación mínima obligatoria:** 50% de los dividendos y utilidades en 180 días desde la declaración.
- **Fase 3 – Repatriación total:** 100% de los activos detectados en 360 días desde la declaración inicial.

### **5. Liquidación de divisas**

- Al menos el **30% de las divisas repatriadas** deberá liquidarse en el mercado local para fortalecer reservas internacionales.

- El restante podrá reinvertirse en proyectos estratégicos nacionales aprobados por la autoridad competente.

## **6. Auditoría y seguimiento**

- Las entidades deberán someter sus informes a **auditoría externa independiente**, con publicación obligatoria en **datos abiertos**.
- El organismo regulador podrá **requerir auditorías extraordinarias** para filiales y activos en paraísos fiscales hasta verificar cumplimiento total.

## **7. Sanciones por incumplimiento**

- **Multas escalonadas:**
  - 1–30 días de retraso: 10% del monto pendiente.
  - 31–90 días: 25% del monto pendiente.
  - 90 días: 50% del monto pendiente.
- Suspensión temporal de acceso a subsidios, contratos públicos o financiamiento estatal.
- Bloqueo preventivo de nuevas filiales o inversiones externas hasta cumplir obligaciones de repatriación.
- Publicación obligatoria de incumplimientos en registros abiertos y auditables por la ciudadanía.

## **8. Incentivos para cumplimiento voluntario**

- Reducción del 50% de la multa si la repatriación se realiza **antes del plazo máximo asignado**.
- Acceso preferencial a nuevos contratos estratégicos del Estado para empresas que cumplan en tiempo y forma.

### **Artículo 6° — Principios rectores**

Los organismos alcanzados deberán regirse por los siguientes principios:

1. **Transparencia activa.**
2. **Interoperabilidad.**
3. **Soberanía digital.**
4. **Seguridad y protección de datos sensibles.**
5. **Ética, equidad y no discriminación algorítmica.**
6. **Participación ciudadana y auditoría social.**
7. **Eficiencia fiscal y sostenibilidad.**
8. **Trazabilidad completa de procesos, decisiones y datos.**
9. **Apertura por defecto, salvo excepciones justificadas.**

### **Artículo 7° — Definiciones**

A los fines de esta ley se entiende por:

- a) **Datos abiertos:** información pública publicada en formatos no propietarios, accesibles, gratuitos, interoperables y reutilizables (.csv, .json, API).
  - b) **Interoperabilidad:** capacidad técnica y semántica que permite que los sistemas públicos intercambien información entre sí sin fricciones.
  - c) **Datos sensibles:** aquellos cuya publicación pueda afectar la seguridad nacional, integridad de las personas o derechos fundamentales.
  - d) **Datos soberanos:** datos generados por organismos públicos, financiados por fondos públicos o estratégicos para la Nación.
  - e) **Trazabilidad:** registro verificable y auditabile del ciclo completo del dato, desde su origen hasta su uso final.
  - f) **Algoritmos y modelos de IA públicos:** sistemas desarrollados o adquiridos mediante recursos estatales.
  - g) **Tokenización ética:** proceso de representación digital verificable de un activo público, procedimiento o dato bajo estándares éticos, auditables y no especulativos.
- 

## **TÍTULO II — GOBERNANZA NACIONAL DE DATOS SOBERANOS: CREACION DE LA ANDAS Y DEL PORTAL NACIONAL DE DATOS ABIERTOS Y SOBERANOS.**

### **Artículo 8° — Creación de la ANDAS**

Créase la Agencia Nacional de Datos Abiertos y Soberanos (ANDAS), como organismo autárquico, descentralizado y confederal, con autonomía técnica, funcional, financiera y administrativa, bajo la órbita de la Jefatura de Gabinete de Ministros, pero con gobernanza federal y paritaria entre Nación, provincias y universidades públicas.

La ANDAS será la **autoridad de aplicación** de la presente ley, actuando como ente rector en materia de **gobierno abierto, soberanía tecnológica, interoperabilidad estatal, ética digital y protección de datos públicos**.

La ANDAS tendrá **sede rotativa y desconcentrada**, pudiendo establecer su **Consejo Federal Permanente** en distintas regiones del país conforme al principio de equidad territorial.

Sus oficinas principales estarán distribuidas de manera equitativa entre las **cinco regiones federales** (Norte, Centro, Cuyo, Patagonia y Litoral), funcionando en red con las

universidades nacionales, los polos tecnológicos y las agencias provinciales de innovación.

**Ejercer su autoridad de aplicación bajo un modelo de gobernanza confederal**, garantizando la participación efectiva de las provincias, universidades y organizaciones sociales en la toma de decisiones estratégicas.

El **Consejo Federal de Datos Abiertos y Ética Digital** será el órgano colegiado de dirección, con voto equitativo por región y mecanismos de rotación institucional cada dos años.

#### **Artículo 9° — Funciones.**

La **Agencia Nacional de Datos Abiertos y Soberanos (ANDAS)** tendrá como misión general garantizar la **soberanía digital, la ética en el uso de los datos y la transparencia pública** en todo el territorio nacional.

En cumplimiento de ello, serán sus funciones:

- a) Implementar **políticas nacionales de datos abiertos y soberanos**; promoviendo la publicación, **reutilización y transparencia de la información pública** en formatos abiertos, accesibles y **auditables por la ciudadanía**.
- b) **Administrar el Registro Nacional de Activos Digitales (RNADE)**; que contendrá los datasets, infraestructuras, algoritmos, plataformas, licencias, sistemas y proyectos tecnológicos bajo dominio público, garantizando su trazabilidad, interoperabilidad y resguardo soberano.
- c) **Supervisar el cumplimiento ético y soberano del tratamiento de datos; por parte de los organismos públicos, entidades privadas contratistas, y proveedores tecnológicos del Estado**, conforme a los principios de autodeterminación informativa, proporcionalidad y legalidad.
- d) **Coordinar con AAIP, universidades y sociedad civil; fomentando la participación ciudadana**, la transparencia activa y la **formación en derechos digitales**.
- e) **Promover estándares de interoperabilidad, transparencia y seguridad, basados en software libre y estándares abiertos** (OAuth2, OpenID, DCAT-AP-AR, RDF, TLS 1.3, AES-256), asegurando el cumplimiento de **normas internacionales y la soberanía tecnológica argentina**.
- f) **Emitir certificaciones éticas, tecnológicas y ambientales** para proyectos, plataformas y servicios digitales estatales o mixtos, garantizando su compatibilidad con la presente ley y con los principios de sostenibilidad, accesibilidad y justicia algorítmica.

- g) **Impulsar la creación de Nodos Regionales de Innovación Abierta**, laboratorios de gobierno, hackathons federales y programas de colaboración entre Estado, ciudadanía, universidades y empresas nacionales, promoviendo el desarrollo de tecnologías soberanas y éticas.
- h) **Elaborar y actualizar el Código Ético Nacional de Inteligencia Artificial y Datos Abiertos**, de aplicación obligatoria para toda entidad pública o contratista que emplee inteligencia artificial, algoritmos predictivos o sistemas automatizados de decisión.
- i) **Administrar el Fondo de Innovación Soberana (FIS)**, destinado a financiar proyectos públicos, cooperativos o privados vinculados a inteligencia artificial ética, desarrollo tecnológico nacional, sostenibilidad digital y economía circular.
- j) **Supervisar la Defensoría Nacional de Derechos Digitales (DNDD)** y garantizar canales efectivos para denuncias ciudadanas sobre vulneraciones de privacidad, vigilancia indebida, o prácticas tecnológicas abusivas.
- k) **Asegurar la gobernanza confederal y federal de la ANDAS**, con representación equitativa y rotativa de las provincias, universidades y actores sociales en la toma de decisiones estratégicas.
- l) **Auditar algoritmos y sistemas automatizados** utilizados en el sector público.
- m) Supervisar el cumplimiento del **Mecanismo Nacional de Auditoría Ciudadana Digital (MACD)**.
- n) Evaluar **riesgos de concentración digital**, dependencia tecnológica y **vulnerabilidades críticas**.
- o) **Elaborar reportes trimestrales públicos de avance e impacto fiscal**.
- p) Coordinar **asistencia internacional** con ONU, CEPAL, UNESCO, BID, CAF y OGP.

El Archivo Nacional de Datos Abiertos y Soberanos (ANDAS) establecerá y administrará el **Régimen Nacional de Clasificación y Desclasificación de la Información Pública**, en coordinación con los organismos competentes en materia de defensa, seguridad, ciencia, tecnología y derechos humanos.

Artículo 7° — Procedimiento ciudadano de acceso, revisión y control de la reserva de información

## 1. Derecho ciudadano de acceso

Toda persona, física o jurídica, nacional o extranjera, tiene derecho a **solicitar y recibir información pública** sin necesidad de acreditar interés directo ni justificación del pedido, conforme al **principio de máxima publicidad y ley de derecho a la**

## **información.**

Las solicitudes podrán realizarse por medios electrónicos, presenciales o postales ante el organismo competente, y deberán ser gratuitas.

### **2. Plazos y respuesta obligatoria**

El organismo requerido deberá responder en un plazo máximo de **quince (15) días hábiles**, prorrogables por única vez por **diez (10) días hábiles adicionales**, mediante acto fundado.

La falta de respuesta en dicho plazo se considerará **silencio administrativo negativo**, habilitando al solicitante a recurrir ante el **ANDAS** o el **órgano garante del derecho de acceso a la información pública**.

### **3. Denegación o reserva de información**

En caso de denegarse total o parcialmente el acceso, el funcionario responsable deberá emitir un **acto administrativo formal**, que contenga:

- a) la identificación de la norma legal específica que habilita la reserva;
- b) los motivos técnicos y jurídicos concretos;
- c) el nivel y plazo de clasificación de la información;
- d) el nombre y cargo del responsable de su custodia;
- e) la indicación expresa de los **recursos disponibles para la revisión del acto**.

Dicho acto deberá notificarse al solicitante y remitirse al **ANDAS** dentro de los **cinco (5) días hábiles** de dictado.

### **4. Recurso de revisión ante el ANDAS**

El solicitante podrá interponer, dentro de los **quince (15) días hábiles** de notificada la denegatoria o vencido el plazo de respuesta, un **recurso de revisión** ante el **Archivo Nacional de Datos Abiertos y Soberanos (ANDAS)**.

El ANDAS deberá evaluar:

- la legalidad y proporcionalidad de la reserva;
- la correspondencia con los criterios de seguridad y defensa definidos en el artículo 2;
- y la posible existencia de un **interés público prevalente** que justifique la desclasificación total o parcial.

El ANDAS resolverá en un plazo máximo de **treinta (30) días hábiles**, pudiendo requerir informes técnicos, dictámenes jurídicos o audiencias públicas cuando lo considere necesario.

## **5. Recurso jerárquico y control legislativo**

Si el ANDAS confirma la reserva, el solicitante podrá interponer un **recurso jerárquico** ante la **Comisión Bicameral de Información y Transparencia del Congreso de la Nación**, que actuará como última instancia administrativa.

Dicha Comisión podrá solicitar informes al Poder Ejecutivo, disponer la desclasificación o requerir la intervención del **Defensor del Pueblo** o la **Auditoría General de la Nación** cuando el interés público lo amerite.

## **6. Garantías contra represalias o censura**

Ninguna persona podrá ser perseguida, sancionada o discriminada por ejercer su derecho a solicitar información o cuestionar un secreto de Estado.

Todo acto de represalia o intento de censura constituirá **violación a los derechos de libertad de expresión y acceso a la información pública**, sancionable conforme al Código Penal y la Ley de Ética Pública.

### Artículo 10º — Transparencia Cívica Soberana y Control Social

Créase en el ámbito del ANDAS el **Régimen Federal de Transparencia Cívica Soberana**, destinado a garantizar el ejercicio efectivo del derecho al acceso a la información pública y la rendición de cuentas de los organismos del Estado, empresas con participación estatal y entidades privadas que administren fondos públicos o bienes estratégicos de la Nación.

#### **a) Transparencia activa y pasiva.**

Todos los organismos comprendidos deberán publicar y mantener actualizada la información relativa a su gestión, presupuesto, contratación, reservas, endeudamiento, y toda otra materia de interés público nacional, provincial o municipal, en formatos abiertos, auditables y reutilizables.

Ninguna información podrá ser declarada reservada o secreta sin acto administrativo fundado en norma expresa y vigente, con mención del daño concreto que su divulgación produciría y del plazo de la reserva.

#### **b) Publicación automática de reservas de información.**

Todo acto que declare información como “reservada” deberá ser notificado al ANDAS en un plazo no mayor de cinco (5) días hábiles, y publicado en la **Plataforma Federal de Acceso Denegado (PAD)**, indicando el organismo solicitante, la norma invocada y el fundamento del secreto.

La PAD tendrá carácter público y será auditible por la ciudadanía y las universidades nacionales.

#### **c) Consejo Federal de Control Cívico.**

Créase el **Consejo Federal de Control Cívico de la Información Pública**, como órgano autónomo de composición plural e independiente, integrado por:

- representantes de organizaciones sociales y académicas,
- un representante por cada provincia,
- y un miembro designado por sorteo ciudadano cada dos años.

El Consejo tendrá facultades para auditar, dictaminar y recomendar la desclasificación de información cuyo carácter reservado se considere infundado o abusivo. Sus dictámenes serán públicos y deberán ser considerados por el Congreso de la Nación.

**d) Límites del secreto de Estado.**

Solo podrá invocarse el “secreto de Estado” cuando la publicidad de la información represente un riesgo cierto, grave e inmediato para la defensa nacional o la seguridad de las personas, y siempre bajo control parlamentario y revisión del Consejo Federal de Control Cívico.

En ningún caso se considerará comprendida la información vinculada a:

- la gestión presupuestaria,
- las reservas del Banco Central,
- la deuda pública,
- o los actos de gobierno relativos al patrimonio nacional.

**e) Sanciones.**

El incumplimiento injustificado del deber de transparencia o la invocación abusiva del secreto de Estado constituirán falta grave y causal de responsabilidad administrativa y penal conforme la Ley 25.188 de Ética Pública, sin perjuicio de las sanciones que establezca el presente régimen.

**Artículo 11º — Autoridad de coordinación interjurisdiccional**

La ANDAS actuará coordinadamente con:

- Provincias y municipios
- Universidades nacionales
- Organizaciones de la sociedad civil especializadas
- Sector privado tecnológico
- Cooperativas digitales y comunidades open source

---

## **TÍTULO III — REGISTRO NACIONAL DE ACTIVOS Y BIENES ESTRATEGICOS DEL ESTADO (RNADE) GESTIÓN Y PROTECCIÓN**

# **DE DATOS PERSONALES POR EL ESTADO. LOS DERECHOS DIGITALES**

## **Artículo 12º — Creación**

Créase el **Registro Nacional de Activos Digitales del Estado (RNADE)** como inventario público obligatorio de todos los activos digitales financiados con recursos públicos.

## **Artículo 13º — Contenido mínimo**

El RNADE deberá incluir, como mínimo:

- a) Bases de datos públicas (estructura, periodicidad, responsable).
- b) Algoritmos, modelos y sistemas de IA estatales.
- c) Software, plataformas, licencias y sistemas adquiridos.
- d) Infraestructura crítica digital.
- e) Contratos, convenios y proveedores tecnológicos.
- f) Procesos digitalizados y flujos iniciados por entes públicos.
- g) Patrimonio digital histórico y cultural.

## **Articulo 14º — Definición de Bienes Estratégicos:**

Se consideran bienes estratégicos de la Nación:

1. Todas las empresas y sociedades en las cuales el Estado posea participación directa o indirecta, cualquiera sea su porcentaje de propiedad.
2. Todas las entidades privadas que administren fondos públicos, subsidios estatales, concesiones, licencias, recursos críticos o bienes de interés nacional.
3. **Activos internos y externos** de la Nación
4. **Bienes de la Nación estratégicos: Recursos naturales y físicos estratégicos**, reservas internacionales, **infraestructura crítica** logística de redes de transporte, comunicación, seguridad y defensa nacional, **bienes intangibles y tecnológicos incluyendo la propiedad intelectual estratégica**.
5. **Entes reguladores, organismos desconcentrados y agencias nacionales**.
6. **Universidades nacionales** en todo procedimiento financiado con recursos públicos.
7. **Proveedores contratistas** del Estado en aquello que se refiera a datos, sistemas y desarrollos financiados con fondos públicos.
8. Toda institución que **reciba transferencias, subsidios o asistencia del Estado** y genere datos de relevancia pública.

9. Todo **banco nacional o privado, institución financiera o entidad de intermediación de capital que administre fondos públicos**, recursos estratégicos, reservas, divisas o activos en el país o en el exterior.

### **Artículo 15° – Obligación de Transparencia y Datos Abiertos:**

1. Todas las entidades mencionadas en el Artículo 14° deberán brindar información completa, abierta, auditible, trazable y actualizada sobre su gestión, operaciones financieras, contratación de servicios, transferencia de recursos y desempeño estratégico.
2. La información deberá publicarse en **formatos abiertos, interoperables y accesibles**, permitiendo análisis ciudadano, auditorías independientes y fiscalización por los organismos competentes.
3. La condición de entidad privada, sociedad anónima, fundación, consorcio u otra forma jurídica **no exime** del cumplimiento de estas obligaciones.
4. Ninguna estructura societaria, participación indirecta, subsidiaria, joint venture, consorcio o fideicomiso podrá ser utilizada para eludir la transparencia ni para considerar a los bienes estratégicos como privados o fuera del interés público.

### **Artículo 16° – Activos estratégicos externos y reinversión interna**

1. Se consideran **activos estratégicos externos** todos aquellos recursos financieros, inversiones, dividendos o utilidades generadas por empresas con participación estatal o privadas que administren fondos públicos, que se encuentren fuera del territorio nacional.
2. Las entidades mencionadas en el Artículo X de la Ley deberán:
  - a) Registrar y reportar anualmente, en **formato abierto y auditabile**, todos los activos estratégicos que mantengan fuera del país.
  - b) Repatriar un **mínimo del 50% de los dividendos y utilidades** generadas en el exterior para su reinversión en proyectos estratégicos dentro del territorio nacional, incluyendo infraestructura, energía, agroindustria, tecnología y servicios públicos.
  - c) Liquidar al mercado local un **mínimo del 30% de las divisas recibidas** como parte de esta repatriación, contribuyendo así al fortalecimiento de reservas internacionales.
3. Las empresas deberán publicar trimestralmente:
  - Montos repatriados y liquidados
  - Destino de la reinversión interna
  - Flujos de capital pendientes de repatriación
4. El incumplimiento de estas obligaciones será sancionado con:
  - a) Multas proporcionales al monto de activos externos no repatriados
  - b) Suspensión temporal de acceso a subsidios, concesiones o financiamiento público
  - c) Auditorías forzadas por los organismos de control competentes

### **Artículo 17° – Fiscalización y Sanciones:**

1. El incumplimiento de las obligaciones previstas en los Artículos X y Y será sancionado con:
  - a) Multas proporcionales a la magnitud de los fondos públicos o recursos estratégicos administrados.
  - b) Restricciones o suspensión en el acceso a fondos, subsidios, concesiones o licencias estatales.
  - c) Auditorías forzadas e inmediatas por los organismos de control competentes.
2. Las sanciones se aplicarán **independientemente** de cualquier responsabilidad civil, administrativa o penal que corresponda por hechos vinculados a la gestión de bienes estratégicos.

#### **Artículo 18º – Evaluación de Impacto de Datos Abiertos (EIDA).**

Previo a la publicación de cualquier dataset, el organismo responsable deberá realizar una EIDA que identifique riesgos éticos, sociales o de privacidad, conforme a las pautas establecidas por la ANDAS.

#### **Artículo 19º – Prohibición de tratamientos masivos sin control.**

Queda prohibido el uso de tecnologías biométricas o de perfilado sin evaluación de impacto y autorización expresa. Toda cesión entre organismos deberá ser registrada y auditada.

#### **Artículo 20º – Descentralización y sede federal permanente**

- a) La ANDAS adoptará un **modelo confederal descentralizado**, con polos regionales autónomos y capacidad ejecutiva, distribuidos territorialmente para evitar la concentración institucional.
- b) El **Consejo Federal de Datos Abiertos y Ética Digital** designará cada dos años la **sede operativa federal rotativa**, priorizando provincias con infraestructura tecnológica en expansión.
- c) Las decisiones estratégicas deberán tomarse por consenso federal, garantizando **igual voz y voto** a todas las regiones representadas.
- d) Los informes, licitaciones y auditorías de la ANDAS deberán realizarse de manera descentralizada, asegurando transparencia territorial y rendición pública ante los gobiernos locales y las universidades asociadas.

#### **Artículo 21º – Fondo Federal de Soberanía Digital (FFSD)**

Declaráse el **inicio del modelo de federalismo cooperativo real en materia digital**, poniendo fin al esquema centralizado de gestión tecnológica y presupuestaria concentrado en la Ciudad Autónoma de Buenos Aires.

Créase el **Fondo Federal de Soberanía Digital (FFSD)**, instrumento financiero autárquico y descentralizado, administrado por el **Consejo Federal de la ANDAS**, con representación equitativa de las cinco regiones federales del país.

## Objetivo

El FFSD tiene por finalidad **financiar el desarrollo tecnológico soberano, la innovación abierta y la infraestructura digital federal**, fortaleciendo la autonomía de las provincias, universidades públicas y municipios en la ejecución de políticas de datos abiertos, inteligencia artificial ética y conectividad soberana.

## Principios rectores

- a) **Federalismo cooperativo y solidario:** el fondo se regirá por criterios de equidad territorial, población, infraestructura tecnológica y participación ciudadana, priorizando regiones históricamente postergadas.
- b) **Autonomía provincial y universitaria:** los recursos serán ejecutados directamente por las provincias y universidades públicas, sin intermediación administrativa de organismos nacionales centralizados.
- c) **Transparencia y trazabilidad pública:** toda asignación presupuestaria, proyecto o ejecución deberá publicarse en el **Portal Nacional de Datos Abiertos (.gob.ar)**, bajo estándares de datos abiertos (CSV, JSON, RDF).

## Conformación

El FFSD se integrará con los siguientes recursos:

1. El **0,3 % del Presupuesto Nacional de Tecnologías de la Información y las Comunicaciones (TIC)**.
2. Recursos derivados del **Fondo de Innovación Soberana (FIS)**.
3. Aportes voluntarios y cooperación internacional no reembolsable.
4. Multas, sanciones o recuperos aplicados por la **ANDAS** en materia de incumplimiento ético o soberano.

## Distribución y control

- La **distribución de fondos será automática, previsible y auditabile**, conforme a un algoritmo público y abierto aprobado por el **Consejo Federal de la ANDAS**, que determinará los porcentajes regionales.
- Cada provincia deberá crear un **Nodo Provincial de Soberanía Digital**, responsable de la ejecución y rendición pública de los recursos asignados.
- Las universidades nacionales y cooperativas tecnológicas podrán ser **entidades ejecutoras asociadas**.
- Los resultados serán objeto de **auditoría ciudadana y parlamentaria** anual.

A partir de la entrada en vigencia de la presente ley, toda política, inversión o contratación pública en materia tecnológica, de innovación, inteligencia artificial o infraestructura de datos deberá ajustarse al **Principio de Equilibrio Federal**, que establece:

- a) La **prohibición de concentrar más del 25 % del presupuesto digital nacional en la Ciudad Autónoma de Buenos Aires** o su área metropolitana.
- b) La **obligación de distribución territorial progresiva** de recursos, infraestructura y servicios digitales en las cinco regiones federales del país.
- c) La **instalación obligatoria de nodos de datos, centros de innovación, servidores y programas educativos digitales** en regiones distintas a la capital nacional, garantizando equidad en el acceso y desarrollo tecnológico.
- d) Toda licitación o convenio público en materia tecnológica deberá incluir un **Índice Federal de Impacto Territorial (IFIT)**, que evaluará su contribución al desarrollo descentralizado y al empleo local.

Con este capítulo comienza el **fin del centralismo digital argentino**. La soberanía tecnológica y la ética pública no pueden depender de una sola ciudad.

Desde ahora, el conocimiento, la innovación y los datos públicos se distribuirán entre todas las regiones, universidades y comunidades del país. Es el **inicio del federalismo cooperativo real**: una Argentina digital, justa y descentralizada.

#### **Artículo 23º – Reconocimiento de los derechos digitales.**

El Estado argentino reconoce los **derechos digitales como derechos humanos fundamentales**, en concordancia con la Constitución Nacional, la Ley N.º 25.326 de Protección de Datos Personales, la Ley N.º 27.275 de Acceso a la Información Pública y los tratados internacionales ratificados por la República.

Estos derechos incluyen, entre otros:

- a) el **derecho a la privacidad y protección** de los datos personales;
- b) el **derecho a la seguridad digital** y a la integridad de la información;
- c) el **derecho a la autodeterminación informativa**;
- d) el **derecho a la neutralidad tecnológica y acceso equitativo a la red**;
- e) el **derecho a no ser objeto de vigilancia** masiva ni decisiones automatizadas sin control humano;
- f) el **derecho a conocer, corregir y eliminar los datos personales almacenados por el Estado**.

#### **Artículo 24º – Protección reforzada de datos financieros personales.**

Ninguna autoridad administrativa, organismo público o entidad financiera, nacional, provincial o municipal, podrá acceder, procesar o cruzar datos financieros personales de

los ciudadanos sin **orden judicial previa, específica y fundada**, emitida por juez competente.

Se consideran datos financieros personales toda información vinculada a movimientos bancarios, billeteras virtuales, impuestos, créditos, beneficios sociales o cualquier otra información que permita inferir el patrimonio o consumo del individuo.

La **Agencia Nacional de Datos Abiertos y Soberanos (ANDAS)**, junto con la **AAIP**, administrarán un **Registro Nacional de Acceso a Datos Financieros (RENADAF)** donde se registrarán todas las solicitudes judiciales y accesos efectuados, garantizando trazabilidad, transparencia y control ciudadano.

El acceso no autorizado constituirá falta grave y violación a los artículos 18, 19 y 43 de la Constitución Nacional y a los artículos 157 bis y 248 del Código Penal.

#### **Artículo 25º – Derecho a la privacidad algorítmica.**

Ninguna persona podrá ser objeto de decisiones automatizadas, evaluaciones crediticias, sociales, fiscales o judiciales basadas exclusivamente en algoritmos o sistemas de inteligencia artificial sin intervención humana y sin posibilidad de revisión, recurso y explicación.

Todo ciudadano tiene derecho a conocer los criterios, variables y ponderaciones que intervienen en los sistemas algorítmicos utilizados por el Estado.

#### **Artículo 26º – Derecho al consentimiento informado digital.**

El consentimiento para el uso de datos personales o financieros deberá ser **libre, previo, informado, específico y revocable**, incluyendo medios digitales seguros para otorgarlo o anularlo, conforme al principio de autodeterminación informativa.

#### **Artículo 27º – Garantía de acceso y alfabetización digital.**

El Estado promoverá la **alfabetización digital universal y el acceso equitativo** a las tecnologías, redes y plataformas públicas, especialmente para personas mayores, zonas rurales y grupos en situación de vulnerabilidad, como condición para el ejercicio pleno de los derechos digitales.

#### **Artículo 28º – Defensoría Nacional de Derechos Digitales.**

Créase la **Defensoría Nacional de Derechos Digitales (DNDD)**, organismo autónomo con capacidad de recibir denuncias, intervenir en amparos digitales, auditar algoritmos públicos y garantizar la protección efectiva de los derechos reconocidos en el presente capítulo.

Su actuación se coordinará con la **ANDAS**, la **AAIP**, el **Ministerio de Justicia y Derechos Humanos** y el **Congreso de la Nación**. Todo este apartado posiciona a Argentina como pionera regional en reconocimiento legal de **derechos digitales al rango de derechos fundamentales del siglo XXI** y al crear por primera vez una **Defensoría Digital** en Argentina.

## Artículo 29º – Consentimiento y control sobre el equipamiento de conectividad doméstica.

Las actualizaciones de firmware, la instalación de sistemas de rastreo, telemetría o **compartición automática de red (“hotspot comunitario”)** en equipos de conectividad domiciliaria (routers, módems, dispositivos IoT) **requerirán consentimiento expreso, informado y revocable del titular del servicio.**

El proveedor de servicios de Internet deberá:

- a) Informar de manera clara, visible y comprensible el alcance de cualquier función que implique compartir conexión o transmitir datos de uso.
- b) Ofrecer al usuario **la opción de desactivar** dichas funciones sin costo, sin penalización ni degradación del servicio.
- c) Abstenerse de recopilar o transferir datos de ubicación, consumo o tráfico generados en la red doméstica sin autorización específica.
- d) Garantizar que las actualizaciones de firmware **no alteren la configuración de privacidad elegida por el usuario.**

Queda prohibida la activación automática o por defecto de redes comunitarias, subredes públicas o canales de telemetría sin consentimiento individual.

El uso no autorizado de la red privada del usuario o la cesión de su ancho de banda sin contraprestación será considerado **práctica comercial abusiva** conforme la Ley N.º 24.240 y violación de la presente ley.

La **ANDAS**, en coordinación con el **ENACOM** y la **AAIP**, supervisará el cumplimiento de esta disposición y podrá ordenar la **desactivación inmediata de funciones comunitarias o de rastreo** que vulneren la privacidad del usuario.

## Artículo 30º - Libertad de elección tecnológica y garantías analógicas

1. Toda persona tendrá derecho a **decidir libremente su nivel de participación** en sistemas digitales, monetarios o tokenizados promovidos por el Estado o por entidades privadas.

Ningún servicio público, subsidio o beneficio podrá condicionarse **exclusivamente** a la utilización de herramientas digitales, tokens, billeteras electrónicas o identidades biométricas.

2. El Estado deberá garantizar siempre **mecanismos analógicos o presenciales equivalentes** para el acceso a derechos, servicios y programas sociales, de modo que ninguna persona quede excluida por falta de conectividad, dispositivos o conocimiento tecnológico.

3. La participación en sistemas de tokenización, economía digital o identidad digital será **voluntaria, informada y revocable** sin perjuicio de los derechos del titular.

4. En caso de interrupción de los servicios digitales, fallas energéticas, ciberataques o emergencias nacionales, se activarán **protocolos de continuidad no digitales**, garantizando la operatividad básica de los servicios públicos y la seguridad ciudadana.

5. El Estado promoverá la **resiliencia digital y energética** mediante copias de seguridad descentralizadas, infraestructura híbrida (digital-física) y programas de alfabetización digital soberana.

## TÍTULO IV — PUBLICACIÓN OBLIGATORIA DE DATOS ABIERTOS, ETICA Y TRANSPARENCIA ALGORITMICA.

### Artículo 31° — Publicación obligatoria

Toda entidad alcanzada por esta ley deberá publicar de manera periódica y estandarizada sus datasets fundamentales en el **Portal Nacional de Datos Abiertos y Soberanos**, administrado por ANDAS.

### Artículo 32° — Contenidos mínimos obligatorios

Los organismos deberán publicar, como mínimo, los siguientes conjuntos de datos:

#### 1. Transparencia fiscal

- a) Presupuesto aprobado, devengado y ejecutado.
- b) Transferencias, subsidios, compras y contrataciones.
- c) Ejecución de programas y obras públicas.

#### 2. Datos institucionales

- a) Estructura orgánica y autoridad responsable.
- b) Remuneraciones, escalafón y dotación de personal.
- c) Planes estratégicos y reportes de avance.

### 3. Datos públicos esenciales

- a) Educación, salud, ambiente, producción, seguridad, justicia.
- b) Indicadores sociales y estadísticas públicas.
- c) Patrones de movilidad y servicios públicos (sin datos sensibles).

### 4. Modelos y algoritmos

- a) Descripción detallada de los sistemas automatizados utilizados.
- b) Documentación técnica obligatoria.
- c) Resultados de auditorías éticas o de impacto.

### Artículo 33º — Frecuencia mínima de actualización

Los datos deberán actualizarse al menos:

- a) Mensualmente para ejecución presupuestaria.
- b) Semanalmente para compras y contrataciones.
- c) Trimestralmente para estadísticas institucionales.
- d) En tiempo real para sistemas automatizados críticos.

### Artículo 34º — Formatos permitidos

Los datos deberán publicarse obligatoriamente en formatos abiertos:

- .csv
- .json
- .xml
- API REST
- Metadatos estandarizados (DCAT-AP / Schema.org)

Quedan prohibidos:

- PDF como único formato
- Imágenes, capturas o formatos no reutilizables

### Artículo 35º — Trazabilidad del dato

Cada dataset deberá incluir:

- a) Fecha de creación, actualización y responsable institucional.
- b) Cadena de custodia.
- c) Historial de modificaciones.
- d) Registro automático de accesos y descargas.

### Artículo 36º – Registro Nacional de Activos Digitales (RNADE).

Se inscribirán todos los sistemas, bases, algoritmos y plataformas financiadas con recursos públicos.

**Artículo 37° – Acceso y reutilización.**

Los datos abiertos podrán ser reutilizados con fines de innovación, educación e investigación, garantizando siempre la integridad y veracidad.

**Artículo 38° – Auditoría algorítmica.**

Toda aplicación o sistema que procese datos públicos será sometido a auditorías éticas para prevenir sesgos o manipulación.

**Artículo 39° – Registro Nacional de Algoritmos.**

Se crea un registro público de algoritmos que usen datos con fines de análisis social, político o comercial.

**Artículo 40° – Prohibición de manipulación informativa.**

Se prohíbe el uso de datos públicos para segmentación o manipulación electoral.

**Artículo 41° - Transparencia activa y acceso equitativo a la información pública**

Crease y adecuace el **Portal Nacional de Datos Abiertos (.gob.ar)** bajo software libre (CKAN/Drupal). El actual Portal Nacional de Datos Públicos (datos.gob.ar) será **actualizado y migrado progresivamente a una infraestructura de software libre 100 %, con auditorias independientes eticas y tecnicas trimestrales y de acceso libre**, con código fuente publicado bajo licencia abierta, hospedado en servidores nacionales gestionados por ARSAT y la ANDAS.

**La Agencia Nacional de Datos Abiertos y Soberanos** será la autoridad responsable de su mantenimiento, interoperabilidad y certificación de soberanía tecnológica, **elevando al portal de datos publicos a rango legal**, y además lo **reconstruye bajo soberanía tecnológica**. A su vez, fomentaría la **participacion ciudadania a nivel de interaccion, seguimiento y auditoria ciudadana en tiempo real**, en vez de solo la pasividad actual de las descargas.

**Publicación automática mediante APIs desde los sistemas de gestión estatales.**

La Agencia Nacional de Datos Abiertos y Soberanos (ANDAS) desarrollará e implementará el **Bus Nacional de APIs Públicas (BNAP)**, que permitirá la actualización automática y continua de los datos abiertos desde los sistemas de gestión del Estado Nacional.

Cada organismo deberá exponer, bajo estándares abiertos (OpenAPI v3.0), interfaces seguras (OAuth2, TLS 1.3) que permitan la transferencia de información en tiempo real al Portal Nacional de Datos Abiertos.

Los datos de presupuesto, contrataciones, obra pública, expedientes y estadísticas deberán sincronizarse de manera automática conforme al calendario técnico aprobado por la ANDAS.

Las publicaciones automáticas estarán sujetas a auditoría técnica y ética, garantizando la protección de datos personales y la integridad de la información. La automatización de los datos y su publicación es lo que convierte a esta ley en una herramienta viva de Transparencia proactiva, la cual ya no dependerá de esperar los pedidos de accesos ni de las cargas y voluntades manuales, a su vez trae aparejado **Ahorro administrativo y burocrático** ya que se elimina la duplicación de reportes y planillas, y se logra la **Estandarización nacional debido que** todos los organismos usan un mismo formato técnico. Cumpliendo con una mayor **Prevención de corrupción porque** las contrataciones y presupuestos se pueden auditar en tiempo real y cualquier ciudadano o periodista puede consultar las APIs sin permiso previo.

Los organismos del Estado Nacional deberán publicar sus datos abiertos exclusivamente en **formatos abiertos, interoperables y legibles por máquina**, tales como **CSV, JSON, XML o RDF**, garantizando su libre acceso, reutilización por parte de investigadores, periodistas, emprendedores y ciudadanía en general y compatibilidad con los estándares internacionales de gobierno abierto.

Los metadatos de todos los conjuntos de datos deberán ajustarse al **Perfil de Aplicación de DCAT-AP-AR**, adoptado oficialmente como norma nacional, incluyendo título, descripción, organismo publicador, frecuencia, licencia, cobertura temporal y geográfica, formato y enlace de acceso.

La Agencia Nacional de Datos Abiertos y Soberanos (ANDAS) será responsable de mantener un **Catálogo Nacional de Datos**, validar automáticamente los metadatos y publicar el código fuente del sistema bajo licencia libre. Esto refuerza la soberanía tecnológica al no depender de software privativo.

Ningún organismo podrá utilizar formatos propietarios o cerrados que limiten la transparencia o el acceso equitativo a la información pública.

El Portal Nacional de Datos Abiertos y todos los sistemas bajo la órbita de la Agencia Nacional de Datos Abiertos y Soberanos (ANDAS) deberán cumplir de manera obligatoria (y no solo recomendada) con los **estándares internacionales de accesibilidad web WCAG 2.1 nivel AA**, conforme a lo establecido en la **Ley N° 26.653** y las **normas IRAM 30700**.

La ANDAS, junto con la CONADIS, será responsable de realizar auditorías anuales de accesibilidad, publicando sus resultados y garantizando la participación ciudadana en la mejora continua del portal y sus herramientas digitales.

La Agencia Nacional de Datos Abiertos y Soberanos (ANDAS) llevará a cabo **auditorías públicas trimestrales** para verificar el cumplimiento de los estándares técnicos, éticos, de soberanía y accesibilidad establecidos en la presente ley.

A tales fines, créase el **Sistema Nacional de Auditoría de Datos Abiertos (SINADA)**, que publicará de manera abierta y verificable los resultados de cada auditoría, incluyendo un índice de cumplimiento por organismo público.

Las auditorías evaluarán la vigencia de los formatos abiertos, la calidad de los metadatos, la frecuencia de actualización, el cumplimiento del estándar DCAT-AP-AR, la protección de datos personales, la soberanía tecnológica y la accesibilidad web (WCAG 2.1 AA).

Los resultados serán de acceso libre y deberán publicarse en el Portal Nacional de Datos Abiertos, acompañados de un sistema de observaciones ciudadanas y un canal de reclamos ante la ANDAS.

En caso de incumplimiento reiterado, la ANDAS notificará a la Jefatura de Gabinete y a la Auditoría General de la Nación (AGN) para la adopción de medidas correctivas o sancionatorias.

Los informes trimestrales de cumplimiento constituirán documentos públicos oficiales y deberán conservarse por un período mínimo de cinco (5) años, accesibles para toda la ciudadanía y organismos de control. Este control continuo y verificable del cumplimiento de la ley es de gran ayuda para la prevención de la opacidad de portales oficiales, fomentar la participación ciudadana en la transparencia y control social de datos, generando una mejora continua, confianza y trazabilidad de proyectos públicos y privados.

La ANDAS será la autoridad de aplicación responsable de emitir y mantener actualizado el **Catálogo Nacional de Clasificación de Datos Públicos**, definir los criterios de anonimización, y realizar auditorías éticas y técnicas de cumplimiento en todos los organismos del Estado.

---

## TITULO V - INFORMACION CLASIFICADA POR SEGURIDAD NACIONAL

### Articulo 42° - Límites y excepciones a la apertura de datos. Régimen de clasificación, desclasificación y defensa soberana.

La apertura, publicación y reutilización de datos públicos deberá realizarse respetando los principios de **seguridad nacional, protección de datos personales, confidencialidad debidamente fundada y derechos fundamentales de las personas**, conforme a la legislación vigente en materia de acceso a la información pública y protección de datos.

## **Articulo 43° - Criterios jurídicos del secreto de Estado**

Solo podrá considerarse “**secreto de Estado**” aquella información cuya divulgación **acredite de manera objetiva y fundada** un riesgo cierto y grave para:

- a) la **defensa nacional o la integridad territorial**;
- b) la **seguridad pública en operaciones en curso**, debidamente documentadas; o
- c) la **protección de infraestructuras críticas estratégicas**, previa certificación técnica del organismo competente.

En ningún caso podrán ser clasificadas como secretas las informaciones que:

- revelen o **encubran actos de corrupción**, violaciones a derechos humanos, irregularidades administrativas o uso indebido de fondos públicos;
- **impidan el control** legislativo, judicial o ciudadano sobre la gestión del Estado;
- refieran a estadísticas, presupuestos, contrataciones, convenios, licitaciones o adquisiciones públicas, salvo por razones de seguridad debidamente fundadas y limitadas en el tiempo.

Toda declaración de secreto deberá:

- **Basarse en dictamen técnico y jurídico** emitido por el organismo competente;
- **Indicar su fundamento legal preciso**, el nivel de clasificación, su **plazo máximo de vigencia** y los **criterios de revisión**;
- Ser notificada al ANDAS, al órgano garante del acceso a la información pública y a la Comisión Bicameral del Congreso para su control;
- Ser automáticamente **revisada o desclasificada** cuando cesen las causas que motivaron su reserva o al vencer el plazo establecido.

## **Articulo 44° - Transparencia y control sobre presupuestos reservados**

Los **fondos y partidas presupuestarias clasificadas o de carácter reservado** deberán registrarse en el **Sistema Nacional de Presupuesto Público** y reportarse al **ANDAS** con un nivel de metadatos que preserve la seguridad operativa sin vulnerar el control democrático.

El monto total, objeto, organismo ejecutor y fuente de financiamiento de dichas partidas deberán ser **de conocimiento público**, quedando únicamente bajo reserva los detalles operativos cuya divulgación implique un riesgo demostrado para la seguridad nacional.

Todo gasto reservado estará sujeto a **auditoría posterior de la Auditoría General de la Nación** y al **control parlamentario**, con obligación de remitir informes anuales de ejecución y justificación de reserva.

## **Principio general**

En caso de duda, **prevalecerá el principio de máxima transparencia y soberanía informacional**, que impide la clasificación abusiva o arbitraria de datos públicos y garantiza el derecho ciudadano a la información como pilar del Estado democrático.

## **Articulo 45° - Definición de defensa nacional**

A los fines de la presente ley, se entenderá por **defensa nacional el conjunto de políticas, recursos, acciones y capacidades destinadas a garantizar la integridad del territorio, la protección del pueblo argentino, la preservación de los recursos naturales estratégicos, la infraestructura crítica, y la soberanía tecnológica, informacional, alimentaria y energética de la Nación**.

En ningún caso la defensa nacional podrá invocarse para:

- **Resguardar intereses partidarios**, corporativos o personales de funcionarios públicos;
- **Restringir el acceso ciudadano** a información que revele actos de corrupción, violaciones a los derechos humanos o irregularidades administrativas;
- **Ocultar información presupuestaria**, estadística o de gestión pública.

## **Articulo 46° - Niveles de clasificación**

La información pública podrá clasificarse, de manera **excepcional y temporal**, bajo los siguientes niveles:

- **Reservada**: cuando su divulgación pueda afectar operaciones o procesos en curso de seguridad nacional, con un plazo máximo de **cinco (5) años**;
- **Confidencial**: cuando implique riesgo para la integridad de personas o instalaciones críticas, con un plazo máximo de **tres (3) años**;
- **Pública diferida**: cuando deba preservarse temporalmente hasta completarse un proceso administrativo, judicial o técnico, con un plazo máximo de **un (1) año**.

Toda clasificación deberá acompañarse de un **informe técnico y jurídico fundado**, indicar el **plazo exacto de reserva**, el **organismo responsable** y la **fecha de revisión obligatoria**.

## **Articulo 47° - Desclasificación y control democrático**

El ANDAS coordinará con la **Comisión Bicameral de Información y Transparencia del Congreso de la Nación** un **mecanismo de revisión periódica** para la desclasificación automática o anticipada de la información cuando:

- a) hayan cesado las causas de reserva;
- b) haya transcurrido el plazo máximo legal; o
- c) se verifique interés público prevalente.

Asimismo, toda persona física o jurídica podrá solicitar la **revisión o desclasificación** de información clasificada, debiendo el Estado fundamentar de manera expresa su decisión de mantener la reserva.

#### **Articulo 48° - Principio de proporcionalidad y soberanía democrática**

Toda clasificación deberá interpretarse bajo el principio de **proporcionalidad, temporalidad y mínima restricción**, asegurando que la defensa nacional se oriente a **la protección del pueblo y la soberanía del Estado**, y no al ocultamiento de información de interés público.

La **reserva o confidencialidad de información pública** será siempre **excepcional, temporal, proporcional y fundada**. Ningún organismo ni funcionario podrá invocar el carácter de **secreto de Estado**, confidencialidad o interés institucional para restringir información cuya divulgación resulte necesaria para el control ciudadano, la rendición de cuentas o la prevención de actos de corrupción.

#### **Articulo 49° - Prohibición de leyes o actos de censura (“leyes de mordaza”)**

Queda expresamente prohibida la emisión o aplicación de **normas, reglamentos, directivas internas o acuerdos administrativos** que impongan restricciones genéricas o indefinidas a la comunicación, publicación o acceso a la información pública bajo pretexto de seguridad institucional o estabilidad política.

Cualquier disposición de este tipo será **nula de nulidad absoluta**, por contrariar los principios de **publicidad de los actos de gobierno, libertad de expresión y soberanía informacional del pueblo argentino**, conforme al artículo 33 de la Constitución Nacional y a los tratados internacionales de derechos humanos con jerarquía constitucional.

#### **Articulo 50° - Justificación del secretismo**

Todo funcionario público que deniegue el acceso a información deberá **emitir un acto administrativo formal y fundado**, en el que conste:

- a) el fundamento jurídico y técnico específico de la reserva;
- b) la norma que habilita dicha reserva;
- c) el plazo máximo de vigencia;
- d) el responsable de su custodia; y
- e) los mecanismos y plazos previstos para su revisión o desclasificación.

Este acto deberá notificarse al solicitante, al **ANDAS** y al **órgano garante del derecho de acceso a la información pública**, en un plazo no mayor de **diez (10) días hábiles** desde la denegatoria.

## **Articulo 51° - Derecho de revisión y control ciudadano**

Toda persona física o jurídica podrá **solicitar la revisión de una reserva o secreto invocado**, ante el ANDAS o el órgano garante del acceso a la información.

Si el fundamento de la reserva no cumple los criterios establecidos por esta ley, el ANDAS podrá **requerir su desclasificación inmediata** y notificar a la autoridad competente o, en su caso, al Congreso de la Nación.

La negativa injustificada o reiterada de funcionarios a justificar el carácter reservado de la información constituirá **falta grave y causal de sanción disciplinaria o administrativa**, sin perjuicio de las responsabilidades penales que pudieran corresponder.

## **Articulo 52° - Principio de prevalencia democrática**

En todos los casos, **prevalecerá el principio de máxima publicidad y soberanía informacional**, entendido como el derecho del pueblo a conocer, auditar y deliberar sobre la información producida con recursos públicos, como base de la democracia participativa y del control social sobre el Estado.

## **Articulo 53° - Derecho ciudadano de acceso**

Toda persona, física o jurídica, nacional o extranjera, tiene derecho a **solicitar y recibir información pública** sin necesidad de acreditar interés directo ni justificación del pedido, conforme al **principio de máxima publicidad**.

Las solicitudes podrán realizarse por medios electrónicos, presenciales o postales ante el organismo competente, y deberán ser gratuitas.

## **Articulo 54° - Plazos y respuesta obligatoria**

El organismo requerido deberá responder en un plazo máximo de **quince (15) días hábiles**, prorrogables por única vez por **diez (10) días hábiles adicionales**, mediante acto fundado.

La falta de respuesta en dicho plazo se considerará **silencio administrativo negativo**, habilitando al solicitante a recurrir ante el ANDAS o el **órgano garante del derecho de acceso a la información pública**.

## **Articulo 55° - Denegación o reserva de información**

En caso de denegarse total o parcialmente el acceso, el funcionario responsable deberá emitir un **acto administrativo formal**, que contenga:

- a) la identificación de la norma legal específica que habilita la reserva;
- b) los motivos técnicos y jurídicos concretos;
- c) el nivel y plazo de clasificación de la información;
- d) el nombre y cargo del responsable de su custodia;
- e) la indicación expresa de los **recursos disponibles para la revisión del acto**.

Dicho acto deberá notificarse al solicitante y remitirse al **ANDAS** dentro de los **cinco (5) días hábiles** de dictado.

#### **Articulo 56° - Recurso de revisión ante el ANDAS**

El solicitante podrá interponer, dentro de los **quince (15) días hábiles** de notificada la denegatoria o vencido el plazo de respuesta, un **recurso de revisión** ante el **Archivo Nacional de Datos Abiertos y Soberanos (ANDAS)**.

El ANDAS deberá evaluar:

- la legalidad y proporcionalidad de la reserva;
- la correspondencia con los criterios de seguridad y defensa definidos en el artículo 2;
- y la posible existencia de un **interés público prevalente** que justifique la desclasificación total o parcial.

El ANDAS resolverá en un plazo máximo de **treinta (30) días hábiles**, pudiendo requerir informes técnicos, dictámenes jurídicos o audiencias públicas cuando lo considere necesario.

#### **Articulo 57° - Recurso jerárquico y control legislativo**

Si el ANDAS confirma la reserva, el solicitante podrá interponer un **recurso jerárquico** ante la **Comisión Bicameral de Información y Transparencia del Congreso de la Nación**, que actuará como última instancia administrativa.

Dicha Comisión podrá solicitar informes al Poder Ejecutivo, disponer la desclasificación o requerir la intervención del **Defensor del Pueblo** o la **Auditoría General de la Nación** cuando el interés público lo amerite.

#### **Articulo 58° - Garantías contra represalias o censura**

Ninguna persona podrá ser perseguida, sancionada o discriminada por ejercer su derecho a solicitar información o cuestionar un secreto de Estado.

Todo acto de represalia o intento de censura constituirá **violación a los derechos de libertad de expresión y acceso a la información pública**, sancionable conforme al Código Penal y la Ley de Ética Pública.

### **TÍTULO VI — FINANCIAMIENTO Y SOSTENIBILIDAD PRESUPUESTARIA.**

#### **Artículo 59° - Financiamiento**

La implementación de la presente ley y la creación de la **Nube Pública Nacional (NPN)** se financiarán sin incremento del gasto público total, mediante la **reasignación interna**

**de recursos existentes y la captación de fondos de cooperación internacional no reembolsable**, conforme a los siguientes criterios:

**a) Reasignación del presupuesto TIC nacional**

Dispónese la reasignación anual del **cero coma dos por ciento (0,2 %) del gasto en Tecnologías de la Información y las Comunicaciones (TIC)** previsto en el Presupuesto General de la Administración Nacional de cada ejercicio, el cual deberá ser transferido al **Fondo Nacional de Datos Abiertos y Soberanos (FONDAS)**, administrado por la **Agencia Nacional de Datos Abiertos y Soberanos (ANDAS)**.

Estos fondos tendrán destino específico para el desarrollo, mantenimiento y expansión de la infraestructura digital soberana, la capacitación técnica federal, las auditorías públicas, y los proyectos de innovación abierta previstos en la presente ley.

**b) Cooperación internacional no reembolsable**

La ANDAS, en articulación con la Jefatura de Gabinete de Ministros y el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, podrá gestionar **aportes, subsidios y cooperación técnica no reembolsable** provenientes de organismos internacionales y multilaterales, incluyendo pero no limitándose a la **ONU, CEPAL, BID, CAF, OGP y la Unión Europea**, destinados a fortalecer la transparencia, la ética digital, la protección de datos y la soberanía tecnológica de la República Argentina.

**c) Donaciones y contribuciones específicas**

Podrán aceptarse **donaciones, aportes o contribuciones** provenientes de personas humanas o jurídicas, públicas o privadas, nacionales o internacionales, siempre que su aceptación no condicione la independencia, transparencia o soberanía tecnológica de la política pública establecida por esta ley.

**d) Plan de Costos Totales (TCO)**

La ANDAS deberá elaborar anualmente un **Plan de Costos Totales (TCO)** a cinco (5) años, el cual incluirá las proyecciones de inversiones iniciales (**CAPEX**) y costos operativos (**OPEX**), indicadores de eficiencia, ahorro fiscal y metas de desempeño, priorizando la **eficiencia administrativa, sostenibilidad presupuestaria y ahorro estatal**.

**Implementación:**

1. Reasignación del **0,2 % de los presupuestos TIC** existentes de cada organismo.
2. Cooperación internacional **no reembolsable** (ONU, BID, CEPAL, OGP).
3. Medición y publicación de ahorros derivados de la digitalización (papel, horas, personal).
4. Integración con el **Sistema Integrado de Información Financiera (SIDIF)** para seguimiento en tiempo real.

## 5. Reportes públicos de ahorro digital certificados por la ANDAS.

### **Artículo 60° - Principio de sostenibilidad.**

Toda política, programa o infraestructura de datos abiertos, digitalización o soberanía tecnológica deberá regirse por los principios de **eficiencia, austeridad, transparencia y sostenibilidad presupuestaria**, asegurando el uso racional de los recursos públicos y la maximización del valor social.

Las erogaciones derivadas de la presente ley se cubrirán mediante la **reasignación de hasta el 0,2 % de los fondos destinados a Tecnologías de la Información y las Comunicaciones (TIC)** en el Presupuesto General de la Nación, sin incremento del gasto total.

Podrán integrarse además recursos provenientes de **cooperaciones técnicas no reembolsables** de organismos multilaterales, universidades y agencias de cooperación, así como aportes de provincias y municipios adherentes.

Cada proyecto deberá incorporar un **Plan de Costos Totales (TCO)** a cinco (5) años, que incluya inversión inicial, costos operativos y mantenimiento.

### **Artículo 61° - Eficiencia y control del gasto.**

Todos los organismos alcanzados deberán publicar en el **Portal Nacional de Datos Abiertos (.gob.ar)** los presupuestos, contratos, convenios y gastos asociados a proyectos de digitalización, en formato abierto y auditible.

La **ANDAS** y la **Sindicatura General de la Nación (SIGEN)** serán responsables de auditar anualmente la ejecución presupuestaria y emitir un informe público de eficiencia y retorno social de la inversión.

### **Artículo 62° - Reutilización de infraestructura y software libre.**

Los organismos públicos deberán priorizar el uso de infraestructura existente, soluciones basadas en **software libre o de código abierto** y servicios nacionales provistos por **ARSAT** y entidades públicas, antes de contratar a proveedores extranjeros.

Se prohíbe la adquisición de licencias, nubes o servicios externos si existen equivalentes nacionales de igual funcionalidad técnica.

### **Artículo 63° - Responsabilidad ambiental y eficiencia energética.**

Los proyectos, infraestructuras y servicios desarrollados en el marco de la presente ley deberán garantizar la **eficiencia energética, sostenibilidad ambiental y trazabilidad ecológica** en todas las etapas de su ciclo de vida, conforme a los estándares internacionales y las políticas nacionales de desarrollo sostenible.

Los **centros de datos, nodos regionales y plataformas tecnológicas** del Estado deberán mantener un **Índice de Eficiencia Energética (PUE)** igual o inferior a **1,6**, e incorporar progresivamente un **mínimo del 30 % de energía proveniente de fuentes renovables** (solar, eólica, biomasa o hidráulica).

Los proyectos deberán incluir mediciones de consumo eléctrico y reportes públicos anuales de eficiencia.

#### **Artículo 64° - Cumplimiento normativo ambiental**

Las entidades públicas y contratistas deberán cumplir las normas **IRAM-ISO 14001** (Gestión Ambiental) y **IRAM-ISO 50001** (Gestión Energética), incluyendo políticas de reducción de emisiones, ahorro energético, gestión de residuos y mitigación del impacto ambiental de su infraestructura digital.

El cumplimiento será condición para la certificación de proyectos por parte de la **ANDAS** y el **Ministerio de Ambiente y Desarrollo Sostenible**.

#### **Artículo 65° - Red Federal de Economía circular tecnológica y Pasaporte Digital de Equipos del Estado**

Se fomentará la **reutilización, reacondicionamiento y reciclaje de equipamiento tecnológico**, priorizando proveedores y fabricantes que acrediten procesos de **economía circular**, certificaciones ambientales o etiquetado verde nacional.

Los equipos dados de baja deberán entregarse a **programas oficiales de reciclaje tecnológico** gestionados por el **INTI**, universidades públicas o cooperativas certificadas, prohibiéndose su eliminación en vertederos o exportación sin trazabilidad.

La **Agencia Nacional de Datos Abiertos y Soberanos (ANDAS)**, en coordinación con el **Ministerio de Ambiente y Desarrollo Sostenible**, el **INTI** y el **Ministerio de Producción**, impulsará la creación de una **Red Federal de Economía Circular Tecnológica**, destinada al reacondicionamiento, reparación, reciclaje y redistribución equitativa del equipamiento informático estatal.

Los organismos públicos deberán priorizar la **adquisición, mantenimiento y reparación de equipos reacondicionados** en un porcentaje no inferior al **treinta por ciento (30%)** de sus compras anuales de hardware, promoviendo la reducción de residuos electrónicos y la reutilización responsable.

Créase el **Pasaporte Digital de Equipos del Estado**, un registro único que documentará el ciclo de vida, mantenimiento y destino final de todo equipamiento informático, con trazabilidad ambiental y social en formato abierto.

Las cooperativas tecnológicas, universidades públicas y escuelas técnicas podrán participar como **reparadoras o reacondicionadoras acreditadas**, accediendo a beneficios fiscales y programas de formación profesional en sostenibilidad digital.

Los residuos electrónicos (RAEE) generados por el sector público deberán ser tratados exclusivamente por entidades certificadas en economía circular, garantizando su reciclaje o reutilización total.

El incumplimiento de estas disposiciones constituirá **falta grave ambiental y administrativa**, pasible de sanción por la ANDAS y la SIGEN, con obligación de compensación ecológica equivalente.

## Artículo 66° - Lineamientos técnicos de Infraestructura Digital Verde

La Agencia Nacional de Datos Abiertos y Soberanos (ANDAS), en coordinación con el Ministerio de Ambiente y Desarrollo Sostenible, elaborará y actualizará cada dos (2) años los **Lineamientos Técnicos de Infraestructura Digital Verde (IDV)**.

Estos lineamientos deberán:

1. Establecer **criterios técnicos obligatorios** de eficiencia energética, uso de materiales reciclables, gestión de desechos electrónicos y reducción de huella de carbono.
2. Definir **métricas públicas estandarizadas** (consumo energético, emisiones equivalentes de CO<sub>2</sub>, porcentaje de reutilización de equipos, reciclaje de componentes).
3. Crear un **Sistema de Trazabilidad Ambiental Digital (STAD)**, interoperable con el Portal Nacional de Datos Abiertos (.gob.ar), donde cada organismo del Estado deberá registrar el ciclo de vida ambiental de sus infraestructuras tecnológicas (compra, uso, baja, reciclaje).
4. Permitir **auditorías ciudadanas y de organismos técnicos** (ANDAS, SIGEN, AGN, universidades públicas), garantizando transparencia en la gestión energética y ambiental.
5. Publicar anualmente un **Informe Nacional de Infraestructura Digital Verde**, con resultados y comparativas de eficiencia por organismo, accesible en formato abierto y reutilizable.

## Artículo 67° - Incentivos para tecnologicas e inversores y Certificacion Verde

La ANDAS, junto con la **Jefatura de Gabinete de Ministros**, podrá otorgar **certificaciones de “Entidad Digital Verde”** a los organismos que superen las metas de eficiencia, reciclaje y sostenibilidad.

Créase la **Certificación de Entidad Digital Verde (EDV)**, otorgada por la **Agencia Nacional de Datos Abiertos y Soberanos (ANDAS)**, en coordinación con el **Ministerio de Ambiente y Desarrollo Sostenible**, como instrumento de reconocimiento público a las instituciones, organismos o entidades que cumplan los estándares de sostenibilidad, eficiencia energética y trazabilidad ambiental previstos en la presente ley.

a) La certificación se concederá anualmente a los organismos que acrediten:

1. **Índice de Eficiencia Energética (PUE)** igual o inferior a 1,6;
2. utilización mínima del treinta por ciento (30 %) de energía proveniente de **fuentes renovables**;
3. cumplimiento de las **normas IRAM-ISO 14001 y 50001**;
4. **reutilización, reciclaje o reacondicionamiento del setenta por ciento (70 %)** del equipamiento tecnológico dado de baja con trazabilidad registrada en el **Sistema de Trazabilidad Ambiental Digital (STAD)**;
5. publicación abierta de indicadores ambientales y de **huella de carbono digital**.

- b) La **ANDAS** y el **Ministerio de Ambiente** establecerán tres niveles de certificación: **Oro, Plata y Bronce**, según el grado de cumplimiento de los criterios establecidos.
- c) La certificación tendrá una vigencia de un (1) año, renovable previa auditoría técnica y verificación de indicadores.
- d) Los organismos certificados podrán exhibir el **sello “Entidad Digital Verde”** en sus sitios web, documentación oficial y portales públicos, como reconocimiento a su gestión ambiental responsable.
- e) El incumplimiento de los estándares, la falsificación de datos o la falta de actualización de indicadores implicará la revocación inmediata de la certificación y la inhabilitación temporal para nuevas convocatorias o compras tecnológicas bajo el régimen de esta ley.
- f) La **ANDAS** publicará anualmente el **Listado Nacional de Entidades Digitales Verdes**, con sus niveles de certificación y métricas verificadas, en formato abierto y de libre acceso.

j) **Auditoría y transparencia.**

La **ANDAS**, junto con la **SIGEN** y la **AGN**, elaborará un **Informe Nacional de Sustentabilidad Digital** que deberá presentarse anualmente ante el Congreso de la Nación y publicarse en el portal oficial. Dicho informe incluirá datos financieros, ambientales y de impacto social de las políticas de soberanía tecnológica y datos abiertos.

**Artículo 68º — Trazabilidad y sostenibilidad mediante mecanismos de tokenización ética.**

Para garantizar la sostenibilidad digital, ambiental y ciudadana, y promover infraestructuras públicas resilientes y auditables, el Estado reconocerá la **tokenización ética** como un mecanismo tecnológico opcional y complementario que permite:

1. **Asegurar la trazabilidad en tiempo real** de los indicadores ambientales, sociales, económicos y de gestión pública.
2. **Fortalecer la integridad de los datos abiertos**, asegurando que su ciclo de vida (captura, procesamiento, publicación y auditoría) sea verificable mediante tecnologías distribuidas y mecanismos de consenso transparentes.
3. **Impulsar modelos de sostenibilidad medible**, en los que diferentes variables (emisiones, consumos, presupuestos verdes, gestión de residuos, uso del agua, programas sociales, entre otros) puedan vincularse a sistemas de tokenización ética definidos en normativa específica.

4. **Garantizar que toda tokenización vinculada a datos públicos cumpla estrictamente con principios de ética digital, interoperabilidad, privacidad ciudadana, minimización de datos y descentralización responsable.**

La **implementación técnica** de estos mecanismos se regulará en la **Ley de Tokenización Ética**, actuando la presente ley como marco rector de acceso, transparencia y sostenibilidad de la información.

#### Artículo 69° — Eficiencia Administrativa, Interoperabilidad y Ahorro Estatal

Con el fin de modernizar la gestión pública, reducir duplicidades administrativas y optimizar el uso de recursos estatales, establecense los siguientes lineamientos obligatorios:

1. Creación del Bus de Interoperabilidad Estatal (BIE).
  - a. Créase el **Bus de Interoperabilidad Estatal (BIE)** como infraestructura digital unificada destinada a conectar los sistemas, plataformas y bases de datos de los organismos públicos.
  - b. El BIE deberá operar exclusivamente mediante **protocolos abiertos y estándares internacionales**, incluyendo: **OAuth2, OpenID Connect, REST, JSON-LD**, y otros que determine la autoridad de aplicación.
  - c. Su objeto será **eliminar redundancias administrativas**, garantizar que cada dato sea registrado una sola vez y habilitar su consulta segura por organismos autorizados.
  - d. Todo acceso, intercambio o consulta de información deberá registrarse automáticamente en el **Registro Nacional de Interoperabilidad (RNI)**, con trazabilidad completa y mecanismos de control ciudadano.
  - e. El desarrollo, mantenimiento y documentación del BIE serán de **software libre**, deberán estar alojados en la **Nube Pública Nacional** y serán administrados por la **Agencia Nacional de Datos Abiertos y Soberanos (ANDAS)** en coordinación con la **Jefatura de Gabinete de Ministros**.
2. Incorporación total al GDE y tramitación 100 % digital en un plazo máximo de 24 meses.
  - a. Establécese que, dentro del plazo máximo de **veinticuatro (24) meses** contados desde la promulgación de la presente ley, la totalidad de los trámites administrativos del Estado nacional deberán integrarse al **Sistema de Gestión Documental Electrónica (GDE)** o a sistemas compatibles técnicamente con éste.
  - b. Los organismos deberán adoptar el **Expediente Electrónico Unificado**, eliminando el uso de soporte papel y reduciendo costos de archivo, almacenamiento y logística.
  - c. Cada organismo deberá publicar un **Plan de Transición Digital** aprobado por la **Oficina Nacional de Tecnologías de la Información (ONTI)**.
  - d. Toda persona tendrá derecho a acceder a la totalidad de sus trámites y expedientes desde una **única plataforma digital interoperable**, utilizando autenticación segura

mediante el **DNI electrónico** o la **Clave Digital Soberana** que determine la autoridad de aplicación.

3. Fortalecimiento del DNI electrónico y de la firma digital conforme Ley 25.506.

- a. Reconócese al **DNI electrónico** como la **credencial única de identidad digital soberana** para la autenticación en servicios públicos digitales.
- b. Ratíficase la equivalencia jurídica plena entre la **firma digital** y la firma manuscrita, conforme a la Ley 25.506, debiendo promoverse su adopción progresiva en todos los trámites administrativos, judiciales, educativos y de gestión pública.
- c. Créanse **Puntos Federales de Certificación Digital** en universidades públicas, municipios y delegaciones del RENAPER, a fin de garantizar acceso equitativo y federal.
- d. El software de emisión, validación y auditoría de certificados digitales deberá ser **abierto, auditable, documentado y basado en estándares de soberanía tecnológica nacional**.

4. Publicación trimestral de indicadores de eficiencia y ahorro.

- a. La ANDAS, en coordinación con la Jefatura de Gabinete, deberá publicar trimestralmente en el **Portal Nacional de Datos Abiertos** los indicadores de mejora en eficiencia administrativa, incluyendo:
  - i. Ahorro de papel, tiempo administrativo y costos energéticos.
  - ii. Reducción de expedientes físicos.
  - iii. Incremento de interoperabilidad y eficiencia interinstitucional.
  - iv. Nivel de satisfacción ciudadana.
- b. Los informes deberán publicarse exclusivamente en **formatos abiertos**, incluyendo **CSV** y **JSON**, y ser plenamente accesibles para auditoría ciudadana, periodística y control legislativo.

## TÍTULO VII - PREVENCIÓN DE CONCENTRACIÓN DIGITAL Y AUDITORÍA CIUDADANA DIGITAL (MACD)

[Artículo 70° — Estrategia de soberanía tecnológica](#)

El Estado deberá priorizar:

- a) Software libre y estándares abiertos.
- b) Infraestructura tecnológica soberana.
- c) Modelos de IA nacionales o auditables.
- d) Independencia respecto de proveedores monopólicos.

## **Artículo 71° — Transparencia en contratos tecnológicos**

Todo contrato tecnológico deberá publicarse con:

- a) Montos, cláusulas, alcances y plazos.
- b) Dependencias técnicas generadas.
- c) Requisitos de interoperabilidad.
- d) Condiciones de salida (exit clauses).

## **Artículo 72° — Proveedores tecnológicos estratégicos**

La ANDAS podrá:

- a) Identificar proveedores críticos con riesgo de dependencia.
- b) Exigir evaluación de riesgo.
- c) Obligar a implementar planes de reducción de dependencia.

## **Artículo 73° — Creación del Mecanismo Nacional de Auditoría Ciudadana Digital (MACD)**

Crease el Mecanismo Nacional de Auditoría Ciudadana Digital (MACD) como sistema federal de participación y control ciudadano sobre:

- presupuestos
- ejecución estatal
- decisiones automatizadas
- diseños normativos
- proyectos de innovación pública

## **Artículo 74° — Funciones**

El MACD deberá:

1. habilitar comentarios ciudadanos en tiempo real,
2. mantener foros moderados de control público,
3. registrar aportes con trazabilidad mediante hashing público,
4. emitir informes trimestrales,
5. garantizar retroalimentación institucional obligatoria,
6. fiscalizar la publicación de datos y algoritmos,
7. coordinar con universidades y organizaciones de sociedad civil.

## **Artículo 75° — Transparencia en sesiones y audiencias**

El Congreso deberá:

- a) transmitir sesiones en formatos interactivos,
- b) habilitar canales de participación digital,
- c) publicar documentos técnicos en tiempo real,
- d) permitir observación remota certificada.

## **Artículo 76° — Panel público de trazabilidad**

Se creará un **Panel Nacional de Trazabilidad Ciudadana** donde será posible:

1. acceder a todos los documentos,
2. verificar cambios legislativos,
3. revisar actividades del Ejecutivo,
4. rastrear ejecución presupuestaria,
5. auditar algoritmos del Estado.

Los datos deberán estar en formatos reutilizables y con API abierta.

## **Artículo 77° — Protección del denunciante digital**

Toda persona que denuncie:

- fallas técnicas,
- riesgos de seguridad,
- irregularidades en sistemas públicos,
- sesgos algorítmicos,

será protegida mediante mecanismos de anonimato y prohibición de represalia

## **Artículo 78° — Coordinación**

El MACD será coordinado por ANDAS y la AAIP, en articulación con:

- Congreso
- Defensoría del Pueblo
- Sociedad civil
- Universidades nacionales

## **Artículo 79° — Innovación Abierta, Colaboración Ciudadana y Desarrollo Tecnológico Nacional**

Con el fin de garantizar la soberanía digital, prevenir la concentración tecnológica, promover la participación ciudadana y fortalecer el ecosistema científico-tecnológico nacional, establecense los siguientes lineamientos de innovación abierta y desarrollo tecnológico soberano.

### **1. Creación de Nodos Regionales de Innovación Abierta.**

a. Créanse los **Nodos Regionales de Innovación Abierta** coordinados por **LabGobAR** (Laboratorio de Innovación Pública) en articulación con **universidades nacionales**, **CONICET**, gobiernos provinciales, cooperativas tecnológicas y organizaciones de la sociedad civil.

- b. Cada Nodo funcionará como **incubadora cívico-tecnológica**, destinada al desarrollo de proyectos de:
  - i. Datos abiertos y transparencia pública.
  - ii. Inteligencia artificial ética.
  - iii. Sostenibilidad ambiental y economía circular digital.
  - iv. Trazabilidad y soluciones de participación ciudadana.
  - v. Interoperabilidad y servicios públicos digitales soberanos.
- c. Los Nodos deberán garantizar **acceso equitativo**, con especial prioridad para regiones con menor infraestructura tecnológica, asegurando participación federal.
- d. Su funcionamiento será documentado y auditado públicamente en el Portal Nacional de Datos Abiertos.

## **2. Programa Federal de Hackathons y Desafíos de Datos Abiertos.**

- a. Establécese un **Programa Anual Federal de Hackathons y Desafíos Cívicos**, organizado por la ANDAS y LabGobAR, utilizando datasets oficiales y temáticas propuestas por provincias y municipios.
- b. Los desafíos deberán alinearse a los siguientes ejes estratégicos:
  - i. Transparencia y control ciudadano.
  - ii. Sostenibilidad ambiental y economía circular.
  - iii. Educación, accesibilidad digital e inclusión.
  - iv. Gobierno abierto e interoperabilidad estatal.
  - v. Salud, transporte y servicios públicos inteligentes.
- c. Podrán participar equipos mixtos conformados por ciudadanos, estudiantes, docentes, investigadores, desarrolladores, cooperativas tecnológicas y organizaciones comunitarias.
- d. Deberá garantizarse un **piso mínimo del 40% de participación de mujeres y diversidades** en cada equipo seleccionado.
- e. El programa se desarrollará en tres etapas:  
**Fase 1:** Lanzamiento nacional y hackathons regionales simultáneos (Norte, Centro, Cuyo, Patagonia).  
**Fase 2:** Evaluación técnica y ética por jurado interdisciplinario (tecnología, sostenibilidad, ética y derechos digitales).  
**Fase 3: Demo Día Federal**, con presentación de prototipos ante organismos públicos y potenciales aliados académicos o productivos.
- f. **Premios y financiamiento:**
  - i. Los proyectos ganadores recibirán financiamiento inicial del **Fondo de Innovación Soberana (FIS)**.
  - ii. Accederán a mentoría técnica de ANDAS y LabGobAR.
  - iii. Podrán ser implementados por organismos públicos con seguimiento de impacto y

trazabilidad.

iv. Todas las soluciones premiadas deberán publicarse con **licencias abiertas** (GPL, MIT, Apache, BSD o Creative Commons).

### **3. Estímulo al Uso de Software Libre y Tecnologías Nacionales.**

a. El Estado nacional y sus entidades descentralizadas deberán **priorizar el uso de software libre o de código abierto** en infraestructura, servicios, gestión administrativa y educación digital.

b. Las licencias recomendadas incluyen **GPL, MIT, Apache, BSD** o equivalentes que garanticen:

- i. Acceso al código fuente.
- ii. Libre modificación y redistribución.
- iii. Auditoría pública de seguridad.

c. Cualquier excepción para el uso de software propietario deberá contar con:

- i. Justificación técnica y de impacto en soberanía tecnológica.
- ii. Aprobación por parte de la ANDAS mediante resolución fundada.

d. Créase el **Catálogo Nacional de Tecnologías Abiertas (CNTA)**, que integrará soluciones de software y hardware libre desarrolladas por:

- i. Universidades nacionales.
- ii. Cooperativas tecnológicas.
- iii. PYMES.
- iv. Organismos públicos.
- v. Comunidades de desarrolladores.

e. Los organismos públicos deberán documentar y publicar en el CNTA todas sus implementaciones, mejoras y adaptaciones, garantizando transferencia tecnológica federal.

f. Los organismos que adopten tecnologías abiertas nacionales podrán recibir **bonificaciones presupuestarias o prioridad en programas de innovación soberana**.

g. Las entidades que desarrollen tecnologías abiertas para el Estado podrán acceder a **beneficios fiscales, créditos blandos** o financiamiento del FIS.

h. Todo software utilizado por el Estado deberá ser **públicamente auditabile**, con mecanismos para detectar vulnerabilidades o puertas traseras.

i. La ANDAS y la ONTI deberán publicar anualmente un **Informe Nacional de Seguridad y Transparencia de Software Público**.

j. Se promoverá la enseñanza de software libre y desarrollo abierto en escuelas técnicas, universidades y programas de alfabetización digital.

k. Se fomentarán alianzas con comunidades locales de desarrolladores para fortalecer la soberanía e independencia tecnológica.

#### **4. Fondo de Innovación Soberana (FIS).**

a. Créase el **Fondo de Innovación Soberana (FIS)** destinado a financiar proyectos de:

- i. Inteligencia artificial ética.
- ii. Servicios digitales soberanos.
- iii. Software libre y tecnologías abiertas.
- iv. Infraestructura digital federal.

b. Las alianzas con el sector privado deberán regirse por contratos de transparencia, sin cesión de propiedad intelectual estatal ni monopolización de datos.

#### **5. Marco Ético y Control Algorítmico Público.**

a. El desarrollo tecnológico deberá ajustarse al marco ético de:

- i. Recomendaciones de UNESCO sobre IA.
- ii. Principios OCDE de IA.
- iii. Carta Iberoamericana de Ética de IA.
- iv. Principios de Soberanía Tecnológica Nacional.

b. Será obligatoria la **Evaluación Ética Algorítmica (EEA)** previa al despliegue de cualquier modelo, sistema predictivo o motor de decisión utilizado por el Estado.

c. Créase el **Registro Nacional de Algoritmos Públicos (RNAP)**, con transparencia sobre:

- i. Código fuente auditabile.
- ii. Datasets utilizados (cuando no incluyan datos sensibles).
- iii. Finalidad del algoritmo.
- iv. Riesgos y salvaguardas.

d. Los modelos no sensibles deberán licenciarse bajo licencias abiertas (MIT, AGPL o CC BY-SA).

e. La ANDAS y el **Comité de Ética de Datos Soberanos** serán autoridades de supervisión, auditoría y evaluación continua.

## **TÍTULO VIII — INTELIGENCIA ARTIFICIAL ETICA Y SOBERANA**

### **Artículo 80° — Principios para la IA soberana**

La inteligencia artificial utilizada por el Estado deberá regirse por los principios de:

- a) ética y derechos humanos,
- b) auditabilidad,
- c) no discriminación,
- d) explicabilidad,
- e) trazabilidad,
- f) soberanía tecnológica y nacional,
- g) seguridad y privacidad por diseño.

### **Artículo 81° — Modelos abiertos y auditables**

Todas las IA aplicadas en:

- gestión pública,
  - decisiones automatizadas,
  - análisis de riesgo,
  - servicios al ciudadano,
- deberán ser **abiertas, transparentes y auditables**, salvo que comprometan seguridad nacional.
- La autoridad deberá publicar:
1. descripción del modelo,
  2. función y riesgo,
  3. métricas principales,
  4. sesgos identificados,
  5. informes de auditoría,
  6. responsables técnicos.

### **Artículo 82° — Infraestructura nacional para IA soberana**

El Estado deberá mantener y expandir una infraestructura nacional para IA:

- a) centros de datos soberanos,
- b) nodos de cómputo distribuido,
- c) estándares abiertos,
- d) repositorios científicos,
- e) conectividad federal.

Se priorizará equipamiento compatible con auditorías independientes y sin telemetría oculta.

### **Artículo 83° — Prohibición de cajas negras**

Queda prohibido el uso de sistemas de IA que:

- a) no puedan auditarse,
- b) no publiquen documentación,
- c) no expliquen decisiones automatizadas,

- d) operen sin trazabilidad,
- e) dependan de infraestructura extranjera sin control soberano.

### **Artículo 84° — IA en seguridad pública**

Toda IA aplicada a:

- vigilancia,
  - reconocimiento facial,
  - análisis predictivo,
  - monitoreo urbano,
- deberá cumplir:

1. estándares reforzados de derechos humanos,
2. auditoría trimestral independiente,
3. publicación obligatoria de métricas de sesgo,
4. prohibición de exportación de datos biométricos,
5. prohibición de vigilancia masiva sin orden judicial.

---

### **Artículo 85° — Principios rectores de IA Etica**

El uso de IA en el Estado deberá regirse por:

1. Ética y no discriminación.
2. Transparencia algorítmica.
3. Prevención de sesgos.
4. Explicabilidad y auditabilidad.
5. Seguridad técnica.
6. Soberanía e independencia tecnológica.

### **Artículo 86° — Registro obligatorio de algoritmos**

Todo algoritmo o sistema de IA utilizado por el Estado deberá inscribirse en el **RNADE**, incluyendo:

- a) Objetivo del sistema.
- b) Base legal habilitante.
- c) Dataset de entrenamiento.
- d) Evaluación de sesgos y riesgos.
- e) Auditorías independientes.
- f) Impacto potencial en derechos humanos.

## **Artículo 87º — Evaluación obligatoria de impacto algorítmico**

Antes de implementar un sistema de IA, el organismo deberá realizar:

- a) Evaluación de impacto en derechos fundamentales.
- b) Evaluación de transparencia y trazabilidad.
- c) Pruebas técnicas de equidad y no discriminación.

El informe se publicará de manera íntegra.

## **Artículo 88º — Prohibiciones**

Queda prohibido:

- a) Utilizar IA para decisiones automatizadas sin supervisión humana vinculante.
  - b) Delegar funciones soberanas críticas en sistemas no auditables.
  - c) Adquirir tecnología opaca o sin acceso a documentación técnica mínima.
  - d) Entrenar modelos públicos con datos sensibles sin base legal y sin consentimiento.
- 

# **TÍTULO IX — PROTECCIÓN DE DATOS BIOMÉTRICOS Y SENSIBLES**

## **Artículo 89º — Carácter estratégico de los datos biométricos**

Declarase de interés público y estratégico nacional la protección integral de los datos biométricos, genéticos, faciales, dactilares, vocales y cualquier dato personal que permita identificar, autenticar o perfilar personas.

Estos datos no podrán:

- a) ser exportados,
  - b) ser cedidos a empresas extranjeras,
  - c) alimentar modelos de IA,
- sin autorización expresa del Estado y sin evaluación de riesgo soberano.

## **Artículo 90º — Prohibición de captura indiscriminada**

Se prohíbe a empresas privadas la recolección masiva de datos biométricos, como escaneo ocular, facial o corporal, sin:

- a) consentimiento informado,
- b) auditoría estatal,
- c) garantías de no-exportación,
- d) registro en el RNADE.

Se incluye expresamente el **caso Worldcoin** como referencia de prácticas no deseadas.

### **Artículo 91° — Exigencias de soberanía en sistemas de identidad**

Todos los sistemas de identidad digital, autenticación, credenciales o validaciones deberán:

- a) alojarse en territorio nacional,
  - b) operar con servidores auditables,
  - c) garantizar cifrado y trazabilidad,
  - d) publicar documentación técnica mínima.
- 

## **TÍTULO X — REGULACIÓN Y TRANSPARENCIA DEL ENTORNO DIGITAL DOMÉSTICO**

### **Artículo 92° — Transparencia sobre CGNAT**

Los proveedores de Internet deberán informar de forma previa, clara y verificable si utilizan **Carrier-Grade NAT (CGNAT)**, incluyendo:

1. implicancias sobre trazabilidad,
2. limitaciones para juegos, videollamadas y servicios profesionales,
3. riesgos de confusión legal o criminal en IP compartida.

El uso no informado se considera **práctica abusiva**.

### **Artículo 93° — Derecho a IP pública dedicada**

Todo ciudadano podrá solicitar una dirección IP pública individual.

Los proveedores deberán otorgarla sin penalidades, cargos abusivos ni requisitos discriminatorios.

### **Artículo 94° — Transparencia en routers y dispositivos de red**

Los dispositivos de red deberán:

- a) informar toda telemetría instalada,
- b) tener telemetría desactivada por defecto,
- c) permitir su deshabilitación completa,
- d) permitir el uso de equipos propios del usuario.

### **Artículo 95° — Prohibición de vigilancia doméstica encubierta**

Se prohíbe la activación por defecto de sistemas como:

- Wi-Fi Sensing
- Motion Sensing
- Monitoreo de actividad basada en señales inalámbricas

Toda recolección no consentida se considerará **dato sensible**.

#### **Artículo 96° — Auditorías de seguridad domiciliaria**

Los routers y dispositivos entregados por proveedores podrán ser auditados por:

- organismos del Estado,
  - universidades públicas,
  - organizaciones de seguridad digital,
  - la ANDAS.
- 

## **TÍTULO XI — ESTÁNDARES INTERNACIONALES**

#### **Artículo 97° — Cumplimiento con ONU, CEPAL y OGP**

Toda política derivada de esta ley deberá alinearse con:

- a) Agenda 2030 – ODS 9, 16 y 17,
- b) Marco de Gobernanza Digital de CEPAL,
- c) Declaración de París de la OGP,
- d) Estándares de transparencia fiscal del FMI,
- e) Recomendaciones OCDE sobre datos abiertos.

#### **Artículo 98° — Cierre de brechas internacionales**

El Estado reconocerá y corregirá los retrasos en:

- a) interoperabilidad,
- b) apertura fiscal,
- c) datos públicos,
- d) infraestructura soberana,
- e) digitalización administrativa.

Se deberán emitir informes anuales de avance y cumplimiento internacional.

#### **Artículo 99° — Cooperación técnica internacional**

La ANDAS podrá firmar convenios con:

- ONU,
- Banco Mundial,
- OCDE,
- CEPAL,
- universidades globales,
- organismos de IA ética.

La cooperación no podrá implicar cesión de datos sensibles ni transferencia de soberanía digital.

---

## **TÍTULO XII — ARMONIZACIÓN NORMATIVA NACIONAL**

### **Artículo 100° — Compatibilidad con leyes vigentes**

La presente ley se aplicará en concordancia con:

- a) Ley 25.326 de Datos Personales,
- b) Ley 27.275 de Acceso a la Información Pública,
- c) Ley 27.078 de Argentina Digital,
- d) Ley 25.467 de Ciencia y Tecnología,
- e) Ley 26.206 de Educación,
- f) Ley de Ciberseguridad que el Congreso dicte.

### **Artículo 101° — Prevalencia soberana**

Cualquier contrato, convenio o instalación tecnológica instalada en territorio argentino deberá ajustarse a esta ley.

Ningún acuerdo podrá:

- a) imponer jurisdicción extranjera,
  - b) exigir transferencia de datos,
  - c) forzar uso de plataformas cerradas,
  - d) limitar la auditoría ciudadana o estatal.
- 

## **TÍTULO XIII — DISPOSICIONES SOBRE RIESGOS DIGITALES**

### **Artículo 102° — Riesgo tecnológico y ambiental**

Todo proyecto digital deberá presentar un análisis obligatorio de:

- a) riesgos de seguridad,
- b) impactos ambientales,
- c) impacto presupuestario,
- d) dependencia tecnológica,
- e) riesgo soberano.

### **Artículo 103º — Protección frente a estafas y delitos digitales**

El uso de infraestructura compartida (como CGNAT) no podrá ser utilizado por los proveedores para:

- a) impedir denuncias,
- b) negar trazabilidad,
- c) eludir colaboración judicial.

Queda establecida responsabilidad objetiva por fallas críticas que vulneren identidad digital del usuario.

### **Artículo 104º — Ciberseguridad en infraestructuras críticas**

Se considerarán infraestructura crítica:

- centros de datos,
- redes ISP,
- plataformas del Estado,
- tecnologías de identidad,
- sistemas de IA del Estado,
- routers instalados en hogares.

Estas infraestructuras deberán someterse a auditorías anuales de seguridad y pruebas de penetración certificadas.

## **TÍTULO XIV — DERECHOS DIGITALES DEL USUARIO**

### **Artículo 105º — Derechos garantizados**

Se reconocen como derechos fundamentales en el entorno digital:

- a) derecho a la conexión segura,
- b) derecho a saber qué datos se recolectan,
- c) derecho a utilizar equipos propios,
- d) derecho a auditoría ciudadana,
- e) derecho a no ser vigilado sin consentimiento,
- f) derecho a identidad digital no interferida por CGNAT,
- g) derecho a trazabilidad clara en delitos informáticos.

## **Artículo 106° — Derecho a desactivar telemetría**

Todo dispositivo de red o equipamiento provisto por los ISP deberá:

1. permitir la desactivación completa de telemetría,
2. mostrar con claridad qué datos envía,
3. garantizar que ninguna función de sensing o monitoreo esté activa por defecto.

## **Artículo 107° — Derecho a documentación técnica completa**

Los proveedores deberán entregar:

- manual técnico completo,
- arquitectura de red asignada,
- especificación sobre NAT, CGNAT o IP pública,
- políticas de retención de datos,
- niveles de latencia esperada.

La falta de documentación será considerada práctica de opacidad digital.

## **Artículo 108° — Derecho a router propio**

El usuario podrá reemplazar el router provisto por el ISP sin penalización económica o técnica.

El ISP deberá garantizar interoperabilidad plena.

---

# **TÍTULO XV — TRANSPARENCIA EN INFRAESTRUCTURA DE RED**

## **Artículo 109° — Informe técnico de ISP de carácter público**

Los proveedores de conectividad deberán publicar trimestralmente:

- a) rangos IP utilizados para CGNAT,
- b) cantidad de usuarios por pool,
- c) mecanismos de trazabilidad,
- d) consumo promedio por nodo,
- e) impacto en latencia,
- f) capacidad de red real vs contratada,
- g) auditorías independientes de seguridad.

## **Artículo 110° — Prohibición de configuraciones ocultas**

Queda prohibido instalar en el hogar del usuario dispositivos que:

- a) recolecten telemetría oculta,
- b) transmitan datos no declarados al ISP,
- c) registren presencia o hábitos,
- d) permitan acceso remoto sin aviso y consentimiento expreso.

### **Artículo 111° — Notificación obligatoria de CGNAT**

Los proveedores deberán notificar por escrito al usuario la existencia de CGNAT y sus limitaciones.

La falta de notificación configura infracción grave.

### **Artículo 112° — Derecho a estabilidad funcional mínima**

Los ISP deberán garantizar niveles mínimos de estabilidad:

- latencia estable,
- ausencia de pérdidas recurrentes,
- trazabilidad verificable,
- acceso funcional a servicios en línea.

El incumplimiento habilita compensación automática.

---

## **TÍTULO XVI – INTEGRIDAD ALGORITMICA, AUDITORIA Y GOBERNANZA HUMANA DE DATOS**

### **Artículo 113° – Integridad Algorítmica en el Tratamiento de Datos Públicos**

Todo algoritmo utilizado para procesar, depurar, validar, anonimizar, clasificar, inferir, visualizar o representar datos provenientes del Estado deberá cumplir con los siguientes requisitos:

1. **Transparencia Metodológica Completa**
  - a) Publicación del método de tratamiento, supuestos estadísticos, estructuras de clasificación, penalizaciones aplicadas, umbrales, modelos predictivos, hiperparámetros y demás criterios técnicos.
  - b) Cualquier cambio metodológico deberá documentarse y publicarse con antelación, garantizando conocimiento público del impacto sobre la interpretación de datos.
2. **Control de Versiones y Registro Público Permanente**
  - a) Cada actualización de algoritmos deberá quedar registrada en un historial

- público con número de versión, fecha, responsable y descripción técnica.
- b) El registro deberá incluir evaluaciones previas y posteriores al cambio, para garantizar que las modificaciones no alteren la realidad estadística ni manipulen indicadores.
3. **Auditoría Externa e Independiente**
- Los algoritmos deberán ser auditados por organismos independientes al menos una vez al año, para verificar ausencia de manipulación, sesgo intencional o adulteración de datos.
- 

#### Artículo 114° – Prohibición de Manipulación Algorítmica de Datos Públicos

Queda terminantemente prohibido:

1. Implementar sistemas algorítmicos que alteren, reescriban, oculten, distorsionen o manipulen datos públicos con fines políticos, partidarios, financieros o institucionales.
  2. Utilizar inteligencia artificial opaca, no auditabile o no explicable para procesos vinculados a:
    - estadísticas oficiales,
    - asignación de recursos públicos,
    - evaluación de programas estatales,
    - selección, priorización o exclusión de beneficiarios.
  3. Aplicar modelos predictivos de impacto social sin evaluación ética previa, matriz de riesgos, participación ciudadana o control de organismos independientes.
- 

#### Artículo 115° – Gobernanza Humana Obligatoria de Sistemas Algorítmicos Públicos

##### 1. Supremacía del Control Humano

Todo sistema algorítmico empleado por el Estado estará subordinado al criterio humano y no podrá ejecutar acciones irreversibles ni vinculantes sin intervención y validación de un operador autorizado.

##### 2. Mecanismos de Corte, Reversión y Revisión Permanente

Los sistemas deberán incorporar:

- mecanismos de detención inmediata,
- reversión de cambios,
- auditoría de integridad,
- bitácoras de decisiones,
- protocolos de revisión periódica multidisciplinaria.

##### 3. Prohibición de Autonomía Creciente

Queda vedada la implementación de infraestructuras que permitan auto-entrenamiento no supervisado, modificación autónoma de parámetros, escalamiento de privilegios o desarrollo de submodelos no autorizados.

#### **4. Responsabilidad Legal del Operador y de la Entidad Pública**

Toda entidad será responsable por:

- garantizar la seguridad algorítmica,
- evitar riesgos de manipulación,
- conservar integridad de datos,
- y asegurar que la IA no sustituya decisiones soberanas del Estado.

## **TÍTULO XVII — TOKENIZACIÓN ÉTICA (RÉGIMEN GENERAL)**

### **Artículo 116° — Principios de tokenización ética**

La tokenización vinculada a obras, datos o identidad deberá:

- a) garantizar autoría verificable,
- b) requerir consentimiento informado,
- c) evitar explotación de datos sensibles,
- d) operar sobre infraestructura segura y auditible.

### **Artículo 117° — Condiciones mínimas para emisión**

Toda creación de:

- certificados digitales,
  - NFTs,
  - títulos académicos,
  - activos de identidad,
  - acreditaciones profesionales,
- deberá realizarse:

1. en infraestructura soberana,
2. sin telemetría oculta,
3. sin interferencia del CGNAT en identificación del autor,
4. con timestamp verificable.

### **Artículo 118° — Protección del creador**

Se considerará agravado el delito de estafa, suplantación o apropiación digital cuando se utilice:

- a) IP compartida para ocultar identidad,
- b) telemetría no consentida,
- c) manipulación del router,
- d) extracción indebida de datos del entorno del hogar.

---

# **TÍTULO XVIII — RESPONSABILIDAD Y PENALIDADES**

## **Artículo 119º — Infracciones leves**

Son infracciones leves:

- a) publicar datos con retrasos,
- b) errores de formato,
- c) incumplimientos menores de interoperabilidad.

Sanciones:

- advertencia administrativa,
- plazos de corrección,
- publicación de la infracción.

## **Artículo 120º — Infracciones graves**

Constituyen infracciones graves:

- a) omisión deliberada de datos públicos,
- b) telemetría oculta,
- c) no notificar uso de CGNAT,
- d) impedir auditoría ciudadana,
- e) negarse a publicar algoritmos utilizados en decisiones públicas.

Sanciones:

- multas,
- suspensión de contratos,
- intervención técnica de sistemas.

## **Artículo 121º — Infracciones muy graves**

Son infracciones muy graves:

- a) exportación de datos biométricos,
- b) cesión irregular de infraestructura soberana,
- c) manipulación oculta de algoritmos,
- d) vigilancia masiva sin autorización judicial,
- e) destrucción deliberada de evidencia digital.

Sanciones:

- multas agravadas,
- inhabilitación,

- denuncia penal,
  - auditoría obligatoria de toda la red.
- 

## TÍTULO XIX — IMPLEMENTACIÓN Y FASES

### Artículo 122° — Implementación escalonada

La implementación se desarrollará en tres fases:

1. **Fase I — Orden y Transparencia (0-12 meses)**
  - normalización de datos,
  - auditoría de infraestructura,
  - publicación de algoritmos existentes.
2. **Fase II — Soberanía e Interoperabilidad (12-24 meses)**
  - integración federal,
  - infraestructura soberana,
  - nodos IA auditables.
3. **Fase III — Ecosistema Abierto (24-36 meses)**
  - APIs nacionales,
  - participación ciudadana plena,
  - auditoría inteligente automatizada.

### Artículo 123° — Indicadores de cumplimiento

Se deberán publicar:

- porcentaje de bases de datos abiertas,
  - APIs operativas,
  - IA auditadas,
  - estabilidad nacional de redes ISP,
  - reportes del MACD,
  - auditorías de ciberseguridad.
- 

## TÍTULO XX — COMPATIBILIDAD FISCAL

### Artículo 124° — Principio de equilibrio fiscal

La implementación deberá ser compatible con:

- a) equilibrio fiscal,
- b) eficiencia de gasto,
- c) superávit sostenible.

Queda prohibida la creación de estructuras con impacto fiscal neto.

#### **Artículo 125° — Fuentes de financiamiento**

La ley se financiará con:

- a) reasignación de partidas existentes,
- b) cooperación internacional no reembolsable,
- c) ahorros por digitalización,
- d) alianzas público-comunitarias,
- e) automatización de procesos.

#### **Artículo 126° — Evaluación fiscal anual**

La ANDAS deberá emitir un informe anual:

- impacto fiscal,
- ahorro generado,
- reducción de CAPEX,
- impacto en costos operativos.

---

## **TÍTULO XXI — DISPOSICIONES FINALES**

#### **Artículo 127° — Reglamentación**

El Poder Ejecutivo dispondrá la reglamentación en un plazo máximo de **180 días**.

#### **Artículo 128° — Vigencia**

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

#### **Artículo 129° — Carácter de ley marco**

Esta ley será la norma madre de:

- Datos Abiertos,
- IA Soberana,
- Soberanía Digital,
- Infraestructura Ética del Hogar,

- Tokenización Ética,
- Auditoría Ciudadana Digital.

## FUNDAMENTOS

La presente Ley tiene como objetivo establecer el régimen jurídico integral para la gestión, apertura, protección y uso soberano de los datos públicos en la República Argentina, reconociendo que los datos públicos son un recurso estratégico para la transparencia, la innovación y el fortalecimiento de la democracia.

En la actualidad, los datos se han consolidado como un activo clave que, si se gestiona adecuadamente, permite la mejora continua de la administración pública, fomenta la eficiencia en el uso de recursos y optimiza la toma de decisiones basadas en información veraz y actualizada. La apertura de datos es, además, un catalizador de la innovación responsable, que promueve el desarrollo tecnológico soberano y la creación de soluciones basadas en la ética y la justicia social.

Esta Ley se inspira en los principios establecidos por los organismos internacionales que promueven el Estado Abierto, como la Organización de las Naciones Unidas (ONU), la Comisión Económica para América Latina y el Caribe (CEPAL) y la Alianza para el Gobierno Abierto (OGP). A través de estas orientaciones, se busca dar cumplimiento a los compromisos asumidos por Argentina en materia de gobierno abierto, acceso a la información pública y la protección de los derechos digitales de sus ciudadanos.

Los datos abiertos no solo deben garantizar el acceso y la disponibilidad pública, sino también asegurar que su uso sea realizado de forma ética, responsable y alineada con los principios de soberanía tecnológica. El marco propuesto en esta Ley contempla la creación de un ecosistema nacional que facilite la interoperabilidad de los datos entre las distintas instancias del sector público, privado y la ciudadanía, promoviendo una participación activa de la sociedad en la toma de decisiones colectivas.

A lo largo de esta Ley se establece que los datos públicos serán abiertos y accesibles en formatos interoperables, promoviendo la transparencia y la trazabilidad de las políticas públicas. El control ciudadano sobre los datos también es central en el diseño normativo, garantizando la audibilidad y la posibilidad de supervisión por parte de la sociedad, a fin de asegurar que los mismos no sean utilizados de manera inapropiada ni vulneren derechos fundamentales.

Uno de los aspectos clave de la Ley es su capacidad para fomentar un entorno propicio para la innovación tecnológica soberana. A través de la apertura de datos públicos, se facilita la creación de herramientas basadas en inteligencia artificial (IA) ética, que garanticen el respeto a los derechos de los ciudadanos, la privacidad y la equidad social. Así, el uso responsable de los datos se convierte en un pilar fundamental para el desarrollo económico, tecnológico y social del país.

En este sentido, la Ley de Datos Abiertos, como marco normativo madre, también regula y promueve la implementación de sistemas de tokenización pública y auditoría ciudadana digital. Estas herramientas permiten garantizar la trazabilidad, la transparencia y la confianza en el uso de los datos, habilitando a los ciudadanos a participar activamente en el control de la gestión pública, asegurando que los datos y la información relacionados con el funcionamiento del Estado sean utilizados para mejorar los servicios públicos y no para fines ajenos al interés general.

El desarrollo de un marco normativo robusto en esta materia no solo responde a la necesidad de una gestión pública más eficiente y moderna, sino que también constituye un avance en el fortalecimiento del Estado de Derecho, promoviendo la equidad y la justicia social a través de la apertura de la información, el acceso a la tecnología y el empoderamiento de la ciudadanía.

Por lo tanto, esta Ley busca sentar las bases para un futuro en el que el uso soberano y ético de los datos públicos sea una herramienta esencial para mejorar la calidad de vida de los ciudadanos, garantizar el acceso a la información pública y asegurar que las políticas públicas se desarrolle de manera transparente, inclusiva y accesible para todos.

**Firmado:**

**Natividad Vidal**

Autora del Proyecto

Capilla del Monte, Córdoba, Argentina

**Firma manuscrita digital:**



Natividad Vidal

DNI 27.716.481

**Correo institucional:**

datosabiertossoberanosar@gmail.com

**Acreditación:**

El presente proyecto es presentado en carácter de autora ciudadana y en cumplimiento de estándares internacionales de Gobierno Abierto, Transparencia Digital y Soberanía de Datos.

# **ANEXO I — PLAN ESTRATEGICO DE IMPLEMENTACION**

Ley de Datos Abiertos, Éticos y Soberanos de la República Argentina

**Duración total del Plan:** 36 meses

**Ejecución supervisada por:** Agencia Nacional de Datos Abiertos y Soberanos (ANDAS)

**Marco metodológico:** CEPAL – OGP – ONU (ODS 16)

---

## **1. Objetivos Estratégicos**

1. Garantizar apertura total de datos públicos no sensibles.
  2. Construir infraestructura nacional soberana y estandarizada.
  3. Crear mecanismos de IA auditables y transparentes.
  4. Reducir CAPEX estatal y mejorar eficiencia operativa.
  5. Democratizar el acceso a información y participación ciudadana.
  6. Alinear la política pública con estándares internacionales.
- 

## **2. Fases de Implementación**

### **Fase I — Orden, Diagnóstico y Transparencia (0–12 meses)**

- Inventario completo de activos digitales del Estado: bases, APIs, algoritmos, servidores.
- Creación operativa del **RNADE** (Registro Nacional de Activos Digitales).
- Publicación inicial de 200 datasets prioritarios (gasto, compras, ambiente, salud, educación).
- Auditoría de prácticas de CGNAT y telemetría por ISP.

- Apertura de algoritmos utilizados para decisiones públicas.
- Implementación del Mecanismo de Auditoría Ciudadana Digital (MACD).

**Resultados esperados:**

- Transparencia inicial garantizada.
  - Identificación de duplicidades y sobrecostos.
  - Primer reporte fiscal de impacto.
- 

**Fase II — Integración Soberana y Estándares Federales (12–24 meses)**

- Normalización de datasets bajo formato CSV/JSON/API REST federal.
- Implementación de nodos federales interoperables con municipios y provincias.
- Construcción de la infraestructura de IA soberana (modelos abiertos auditables).
- Inclusión de universidades, cooperativas digitales y sector privado responsable.
- Estándares nacionales de infraestructura de hogar (routers éticos certificados).
- Soporte nacional para IP pública dedicada y reducción de CGNAT abusivo.

**Resultados esperados:**

- Interoperabilidad federal.
  - Datos en tiempo real de toda la administración pública.
  - Infraestructura digital soberana y auditabile.
- 

**Fase III — Ecosistema Abierto, Inteligente y Resiliente (24–36 meses)**

- Apertura completa de APIs nacionales.
- Integración con sistemas de IA abiertos y nacionales para predicción, eficiencia y auditoría.
- Panel único de trazabilidad fiscal, presupuestaria y ciudadana.
- Certificación anual de calidad de datos y seguridad.
- Integración completa con estándares ONU – CEPAL – OGP.

**Resultados esperados:**

- Ecosistema autosostenible.
  - Reducción sustancial de costos informáticos.
  - Soberanía tecnológica consolidada.
-

# **ANEXO II — EVALUACIÓN ECONÓMICA, FISCAL Y REDUCCIÓN DE CAPEX**

## **1. Ahorros proyectados**

La digitalización y apertura generan beneficios fiscales directos:

<b>Rubro</b>	<b>Ahorro estimado</b>
Eliminación de sistemas duplicados	15–25%
Eficiencia operativa del Estado	10–18%
Reducción de corrupción por trazabilidad pública	20–30%
Optimización de compras públicas	8–12%
Reducción de CAPEX de infraestructura digital	25–40%

## **2. Reducción del CAPEX estatal**

La ley establece que:

- Todo desarrollo financiado con fondos públicos debe registrarse y ser reutilizable.
- Se evita “comprar dos veces” software, API, servidores o sistemas ya existentes.
- Se termina el “ciclo de proveedores cautivos”.

### **Impacto directo:**

El Estado pasa de pagar CAPEX a un modelo de reutilización y mantenimiento (OPEX optimizado).

---

## **3. Equilibrio fiscal**

La ley **no genera gasto neto**, porque:

- Utiliza estructuras existentes (AAIP, JGM, organismos TIC).
  - Reasigna partidas.
  - Aprovecha cooperación internacional no reembolsable.
  - Reduce costos actuales.
-

# **ANEXO III — INCENTIVOS PARA TECNOLÓGICAS E INVERSORES (NO FISCALES)**

## **1. Reducción de conflictos legales**

Apertura controlada = menos litigios.

Empresas gastan millones en defensa de monopolios; este modelo:

- reduce presión regulatoria,
  - mejora transparencia,
  - evita demandas por abuso de posición dominante.
- 

## **2. Menos presión política y de lobby**

Apertura = menores costos de defensa monopólica.

---

## **3. Reputación internacional**

Las empresas abiertas:

- mejoran ESG,
  - ganan confianza,
  - evitan sanciones por opacidad.
- 

## **4. Estrategias complementarias**

1. **Transición gradual de apertura**
  2. **APIs limitadas para desarrolladores**
  3. **Modelos colaborativos Estado–empresa–universidades**
  4. **Integración a programas de IA soberana federal**
-

# **ANEXO IV — INFORME TÉCNICO CIUDADANO SOBRE CGNAT Y ESTABILIDAD**

Documento destinado a respaldar la sección de protección del hogar digital.

Incluye evidencia de:

- pérdidas de paquetes,
- latencias irregulares,
- caídas de conectividad,
- imposibilidad de abrir puertos,
- incompatibilidad con videojuegos online y videollamadas,
- ausencia de notificación previa,
- riesgo potencial para investigaciones de delitos informáticos.

Conclusión:

El uso obligatorio y no informado de CGNAT constituye una vulneración al derecho a la transparencia digital.

---

# **ANEXO V — MARCO INTERNACIONAL (CEPAL – ONU – OGP)**

## **1. Alineación ONU — Agenda 2030**

ODS 9 — Industria, Innovación e Infraestructura  
ODS 16 — Instituciones responsables  
ODS 17 — Alianzas

---

## **2. Estándares CEPAL**

- Infraestructura digital como bien público
- Transparencia fiscal

- Datos abiertos para desarrollo
  - Soberanía tecnológica regional
- 

### **3. Estándares OGP**

- Datos abiertos por defecto
  - Participación en tiempo real
  - Auditoría ciudadana
  - Tecnologías auditables
  - Anticorrupción estructural
- 

## **ANEXO VI — METODOLOGÍA DE TOKENIZACIÓN ÉTICA**

Principios:

1. Autoría verificable
2. Consentimiento informado
3. Transparencia tecnológica
4. Infraestructura soberana
5. No explotación de datos biométricos
6. No interferencia por CGNAT
7. Auditoría criptográfica
8. Metadatos abiertos
9. Validación externa (universidades)
10. Compatibilidad con derechos humanos digitales

Incluye:

- metodología de certificación,
- matrices de trazabilidad,
- criterios de auditoría,
- modelo de licenciamiento soberano,
- criterios de interoperabilidad web3 ética.

## **PROYECTO DE LEY Ley de Tokenización Ética, Soberana y de Alta**

# **Seguridad para Activos, Recursos Estratégicos y Reservas Estratégicas de Argentina – 2025**

**Autora:**

Natividad Vidal

Capilla del Monte, Córdoba, Argentina

**Correo Institucional:** [datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

**Presentado ante:**

Honorable Cámara de Diputados de la Nación

Honorable Cámara de Senadores de la Nación

**Fecha:** \_\_\_\_\_ (colocar al momento de presentación)



Natividad Vidal

DNI 27.716.481

Proyecto presentado para su tratamiento en el marco del Programa de Soberanía Digital Argentina, alineado con estándares ONU – CEPAL – OGP.

# **PARTE I**

- **ÍNDICE GENERAL**
- **TÍTULO I — OBJETO Y ALCANCE**
- **TÍTULO II — PRINCIPIOS RECTORES**
- **TÍTULO III — CLASIFICACION DE INFORMACION PARA TOKENIZACION**
- **TÍTULO IV — TOKENIZACION DE RECURSOS ESTRATEGICOS Y RESERVAS NACIONALES**
- **TÍTULO V — TOKENIZACION DE DATOS BIOMETRICOS Y DATOS SENSIBLES**
- **TÍTULO VI — GOBERNANZA**
- **TÍTULO VII — LICENCIAMIENTO SOBERANO**
- **TÍTULO VIII — INTEGRACION CON OTRAS LEYES**
- **TÍTULO IX — PENALIDADES**
- **TÍTULO X — ARTICULACIÓN CON LOS MINISTERIOS DE SEGURIDAD Y DEFENSA EN SITUACIONES DE EMERGENCIA, CRISIS EXTREMA Y RESERVAS ESTRATEGICAS**
- **TÍTULO XI — PROCEDIMIENTOS OPERATIVOS PARA EMERGENCIAS, CRISIS EXTREMAS Y PROTECCIÓN DE ACTIVOS ESTRATÉGICOS**
- **TITULO XII - INCORPORACIÓN DE ANEXOS TÉCNICOS Y JERARQUÍA NORMATIVA**
- **TÍTULO XIII — INTERVENCIÓN DE ORGANISMOS NEUTRALES INTERNACIONALES EN PROCESOS DE RENEGOCIACIÓN SOBERANA**
- **TÍTULO XIV — AUDITORÍA ESTRATÉGICA SOBRE RECURSOS CRÍTICOS Y ARTICULACIÓN CON DEFENSA NACIONAL**
- **TÍTULO XV — CONTINUIDAD OPERATIVA DEL ESTADO Y PROTECCIÓN DE LA POBLACIÓN EN ESCENARIOS DE CRISIS EXTREMA**
- **TITULO XVI – GOBERNANZA ETICA DE SISTEMAS ALGORITMICOS E INTELIGENCIA ARTIFICIAL**
- **TITULO XVII - TRANSFERENCIA TECNOLÓGICA, AUDITORÍA SOBERANA Y RENEGOCIACIÓN ÉTICA EN SISTEMAS CRÍTICOS**
- **TITULO XVII - DISPOSICIONES TRANSITORIAS Y FINALES**
- **FUNDAMENTOS**

## **PARTE II**

- **FIRMADOS**

## **PARTE III**

- **ANEXO I — SISTEMA DE METRICAS PUBLICAS DE INTEGRIDAD Y ESTAILIDAD ESTRATEGICA (SMPIE)**
- **ANEXO II — METODOLOGIA DE TOKENIZACION SOBERANA Y AUDITORIA MULTICAPA**
- **ANEXO III — ESTANDAR DE PUBLICACION CIUDADANA Y TRANSPARENCIA NO REVELATORIA**
- **ANEXO IV - MÉTRICAS, INDICADORES Y PROTOCOLOS PARA LA TOKENIZACIÓN DE RECURSOS ESTRATÉGICOS Y RESERVAS NACIONALES**
- **ANEXO TÉCNICO V - PROTOCOLOS, INDICADORES Y CAPAS DE SEGURIDAD PARA TOKENIZACIÓN DE DATOS BIOMÉTRICOS Y DATOS SENSIBLES.**
- **ANEXO TÉCNICO VI - GOBERNANZA, RESPONSABILIDADES, FLUJOS DE CONTROL Y SUPERVISIÓN DEL ECOSISTEMA NACIONAL DE TOKENIZACIÓN ÉTICA**
- **ANEXO VII - LICENCIAMIENTO SOBERANO, ESTÁNDARES ABIERTOS, PROTOCOLOS DE NO EXPORTACIÓN Y PROHIBICIÓN DE DEPENDENCIA TECNOLÓGICA**
- **ANEXO VIII. PROTOCOLOS DE PUBLICACIÓN DE SERIES CRÍTICAS DE DATOS EN CONTEXTOS DE EMERGENCIA**
- **ANEXO IX - MODELO DE AUDITORÍA ÉTICA Y TRAZABILIDAD MULTINIVEL (MET)**
- **ANEXO X - MARCO TECNOLÓGICO PARA TOKENIZACIÓN ÉTICA**

# **TÍTULO I — OBJETO Y ALCANCE**

## **Artículo 1° — Objeto.**

La presente Ley establece el **Marco Legal Nacional de Tokenización Ética Estatal**, regulando la representación digital soberana de datos, activos, reservas estratégicas y recursos críticos del Estado, bajo principios de seguridad nacional, ética pública, trazabilidad verificable y control ciudadano no intrusivo.

A los efectos de la presente ley, se entiende por tokenización ética al uso de tecnologías de registro distribuido u otros sistemas digitales de trazabilidad que aseguren transparencia, auditabilidad pública, soberanía de datos, respeto por los derechos humanos, protección ambiental y control estatal efectivo.

## **Artículo 2° — Alcance.**

El régimen de tokenización regulado en esta Ley comprende:

- a) Datos públicos no sensibles.
- b) Datos sensibles y datos biométricos con protección reforzada.
- c) Bienes muebles e inmuebles del Estado.
- d) Infraestructura crítica.
- e) Reservas estratégicas (oro, minerales, energía, biodiversidad, capacidades críticas).
- f) Certificados, títulos, autorías, acreditaciones y cualquier documento público de valor jurídico.
- g) Cualquier otro activo cuya digitalización requiera auditoría, control ético o resguardo soberano.

## **Artículo 3° — Carácter complementario.**

Este régimen es de orden público y se integra con las normas de protección de datos, ciberseguridad, secreto de Estado, acceso a la información, administración financiera y cualquier otra legislación aplicable.

---

# TÍTULO II — PRINCIPIOS RECTORES

## Artículo 4° — Principios rectores.

La tokenización ética estatal se regirá por:

1. **Soberanía digital:** Ningún componente crítico podrá depender de jurisdicción extranjera.
  2. **Transparencia no intrusiva:** Se informan métricas agregadas sin divulgar información crítica.
  3. **Auditoría ciudadana:** Acceso público solo a información no sensible o no reservada.
  4. **No especulación:** Se prohíbe toda forma de cotización, manipulación o uso financiero especulativo de tokens estatales.
  5. **Seguridad nacional:** Protección reforzada ante riesgos geopolíticos, ciberataques y fuga de información estratégica.
  6. **No exportación de biometría:** Prohibición absoluta de transferir, alojar o replicar biometría en terceros países o proveedores extranjeros.
  7. **Infraestructura soberana:** Operación en entornos controlados por el Estado.
  8. **Consentimiento informado:** Todo tratamiento de datos personales requerirá consentimiento expreso, informado y trazable.
  9. **Trazabilidad verificable:** Toda operación deberá generar registros inmutables.
  10. **Ética algorítmica:** Prohibición de algoritmos opacos que puedan vulnerar derechos.
- 

# TÍTULO III — CLASIFICACION DE INFORMACION PARA TOKENIZACION

## Artículo 5° — Categorías de información.

A los efectos de la presente Ley la información se clasifica en:

- a) **Información pública abierta:** Datos no sensibles de libre acceso.
- b) **Información sensible:** Datos cuya divulgación puede afectar derechos individuales o colectivos.
- c) **Información reservada:** Datos operativos que requieren acceso limitado por razones técnicas, económicas o institucionales.
- d) **Información clasificada / Secreto de Estado:** Datos cuya exposición afectaría la seguridad nacional o la posición estratégica del Estado.

## **Artículo 6° — Ejemplos no taxativos.**

- a) **Información pública abierta:** estadísticas no sensibles, indicadores no clasificatorios, normativas, obras públicas visibles.
- b) **Información sensible:** historiales administrativos, datos biométricos, bases ciudadanas, sistemas de pago públicos.
- c) **Información reservada:** existencias estratégicas post-SWIFT, acuerdos tácticos energéticos, inventarios de infraestructura crítica.
- d) **Información clasificada:**
  - Reservas estratégicas de oro, litio y minerales críticos.
  - Localización física de stock estratégico.
  - Detalles operativos de centrales energéticas, torres, fibra óptica o sistemas de defensa.
  - Acuerdos energéticos o tecnológicos con potencias extranjeras que contengan cláusulas de confidencialidad soberana.

## **Artículo 7° — Medición, Auditoría y Publicación de Métricas de Reservas Estratégicas**

### **1. Medición obligatoria.**

La autoridad competente deberá mantener un registro completo, exacto y actualizado de todas las reservas estratégicas del Estado, incluyendo oro, litio, minerales críticos, energía, combustibles, bienes estratégicos y cualquier otro recurso de valor soberano.

### **2. Carácter clasificado.**

Los datos operativos, volúmenes exactos, localización física, rutas logísticas y protocolos de custodia conservarán carácter **clasificado**, y no podrán ser publicados ni divulgados por motivos de seguridad nacional.

### **3. Auditoría soberana obligatoria.**

La medición deberá ser auditada, como mínimo:

- a) Por la autoridad competente del Poder Ejecutivo.
- b) Por la Auditoría General de la Nación.
- c) Por un Comité de Universidades Nacionales con competencia en metrología, seguridad, geología, energía o áreas afines.
- d) Por equipos técnicos acreditados bajo normativa nacional.

### **4. Tokenización ética no replicable.**

Todos los registros deberán tokenizarse bajo mecanismos de integridad no replicable que:

- a) Detecten desvíos automáticamente.
- b) Eviten adulteraciones o pérdidas.
- c) Generen evidencia criptográfica verificable.
- d) Permitan auditorías multicapa sin exponer información clasificada.

### **5. Métricas públicas para control ciudadano.**

Sin exponer información sensible, la autoridad competente deberá publicar indicadores agregados, no revelatorios, que permitan a la ciudadanía evaluar la integridad, estabilidad y coherencia patrimonial del sistema.

Estos indicadores incluirán, como mínimo:

- Índice de consistencia patrimonial (ICP).

- Variación porcentual trimestral de reservas estratégicas.
  - Índice de riesgo sistémico o estrés estratégico.
  - Semáforo de integridad (verde, amarillo, rojo).
  - Alarmas públicas ante anomalías estadísticas o contables.
6. **Periodicidad de publicación.**  
En situaciones normales, la publicación deberá realizarse **cada noventa (90) días**. En contextos de **crisis económica, riesgo de hiperinflación, fuga de capitales o vulnerabilidad financiera** declarada por la autoridad competente, la periodicidad se reducirá a **treinta (30) días**, con obligación de emitir alertas inmediatas al Panel de Trazabilidad Pública ante cualquier anomalía crítica.
7. **Obligación de trazabilidad.**  
La autoridad competente deberá mantener trazabilidad total del proceso, registrando accesos, modificaciones, revisiones, anomalías y dictámenes técnicos.
8. **Responsabilidad administrativa y penal.**  
La alteración, ocultamiento o falsificación de métricas públicas será considerada falta gravísima, sin perjuicio de las responsabilidades penales correspondientes.

#### **Artículo 8° — Tokenización según clasificación.**

La tokenización deberá adaptarse al nivel de riesgo:

- a) **Pública abierta:** Tokenización plena.
- b) **Sensible:** Tokenización con anonimización obligatoria.
- c) **Reservada:** Tokenización basada en indicadores agregados no revelatorios.
- d) **Clasificada:** Tokenización permitida solo bajo modalidad **no replicable**, sin exposiciones externas y con bloqueo de trazas públicas.

---

## **TÍTULO IV — TOKENIZACION DE RECURSOS ESTRATEGICOS Y RESERVAS NACIONALES**

#### **Artículo 8° — Naturaleza de la tokenización.**

Tokenizar NO implica divulgar, publicar, exponer, replicar ni hacer accesible la información original.

Los tokens son representaciones abstractas verificables sin revelar datos críticos.

#### **Artículo 9° — Condiciones para tokenizar reservas estratégicas.**

Se permite tokenizar reservas estratégicas únicamente bajo los siguientes criterios:

- a) Tokenización no replicable.
- b) Infraestructura soberana.
- c) Auditoría en entornos seguros.
- d) Trazabilidad y registro inmutable.
- e) Prohibición expresa de representación 1:1 del volumen físico almacenado.

f) Indicadores públicos solo en formato agregado (tendencias, semáforos de riesgo, estrés sistémico).

**Artículo 10° — Auditoría Técnica Soberana.**

Se establecen **Tokens de Auditoría** que:

- a) Certifican integridad sin revelar datos críticos.
- b) Permiten auditoría multi-capas (técnica, institucional, académica, internacional) sin entregar información clasificada.
- c) Garantizan verificabilidad mediante pruebas criptográficas no intrusivas.

**Artículo 11° — Prohibición de especulación.**

Ningún token generado bajo esta Ley podrá:

- a) Cotizar en mercados.
  - b) Ser utilizado como instrumento financiero.
  - c) Ser objeto de derivados, préstamos, hipotecas o contratos especulativos.
  - d) Funcionar como proxy de reservas estatales.
- 

## **TÍTULO V — TOKENIZACION DE DATOS BIOMETRICOS Y DATOS SENSIBLES**

**Artículo 12° — Prohibición de externalización.**

Queda prohibida la exportación, transferencia, almacenamiento o tratamiento de datos biométricos en proveedores extranjeros o entornos fuera del control estatal.

**Artículo 13° — Entornos controlados.**

Toda tokenización de biometría o datos sensibles deberá realizarse en infraestructura soberana bajo:

- a) Control físico nacional.
- b) Auditorías externas universitarias.
- c) Registro inalterable de accesos.
- d) Segmentación estricta entre entornos públicos y clasificados.

**Artículo 14° — Trazabilidad obligatoria.**

Cada operación deberá generar:

- a) Hash verificable.
- b) Registro de operador.
- c) Motivo de acceso.
- d) Plazo de retención.
- e) Evidencia de consentimiento informado cuando corresponda.

**Artículo 15° — Penalidades agravadas.**

El uso indebido, filtración, replicación o extracción de biometría será considerado falta gravísima con responsabilidad administrativa, civil y penal.

---

## TÍTULO VI — GOBERNANZA

**Artículo 16° — Autoridad de aplicación.**

Será autoridad de aplicación la **Agencia Nacional de Datos Abiertos y Seguridad (ANDAS)** o la entidad que el Poder Ejecutivo determine.

**Artículo 17° — Auditoría Universitaria.**

Las universidades nacionales participarán como auditores externos permanentes, sin acceso a información clasificada, pero con capacidad de evaluar integridad técnica y calidad del proceso.

**Artículo 18° — Panel de Trazabilidad Pública.**

Se crea el Panel de Trazabilidad para información no reservada, encargado de:

- a) Publicar métricas agregadas.
  - b) Detectar riesgos éticos.
  - c) Emitir informes ciudadanos de transparencia.
- 

## TÍTULO VII — LICENCIAMIENTO SOBERANO

**Artículo 19° — Licencias públicas soberanas.**

Toda tecnología, dataset o token producido bajo esta Ley se regirá por licencias soberanas que:

- a) Impidan apropiación extranjera.
- b) Eviten dependencia tecnológica (lock-in).
- c) Exijan auditabilidad del código.

**Artículo 20° — Independencia tecnológica.**

Se establece obligación de:

- a) Software auditabile.
  - b) Infraestructura soberana o híbrida nacional.
  - c) No dependencia de nubes extranjeras.
-

# **TÍTULO VIII — INTEGRACION CON OTRAS LEYES**

Esta Ley se integra con:

- a) Ley de Datos Abiertos Éticos.
  - b) Ley de Sostenibilidad Tecnológica.
  - c) Ley de Ciberseguridad.
- 

# **TÍTULO IX — PENALIDADES**

## **Artículo 21° — Régimen de sanciones.**

La violación del presente régimen implicará sanciones administrativas, civiles y penales.

Se considerarán agravantes:

- a) Riesgo para la seguridad nacional.
  - b) Pérdida de soberanía digital.
  - c) Acceso indebido a información clasificada.
  - d) Exportación o filtración de biometría.
  - e) Manipulación de tokens vinculados a recursos estratégicos.
- 

# **TÍTULO X — ARTICULACIÓN CON LOS MINISTERIOS DE SEGURIDAD Y DEFENSA EN SITUACIONES DE EMERGENCIA, CRISIS EXTREMA Y RESERVAS ESTRATÉGICAS**

## **Artículo 22°. Cooperación Obligatoria con el Ministerio de Seguridad y el Ministerio de Defensa**

El Sistema de Tokenización Ética de Activos y Datos Críticos Soberanos establecerá mecanismos permanentes de coordinación con el Ministerio de Seguridad y el Ministerio

de Defensa para garantizar la integridad, continuidad operativa, trazabilidad y protección de los activos estratégicos de la Nación.

Esta coordinación será obligatoria en los siguientes supuestos:

- a) Amenazas a la seguridad nacional con riesgo de fuga, apropiación, deterioro o bloqueo de reservas estratégicas.
  - b) Escenarios de crisis humanitaria, emergencia social, desabastecimiento crítico o colapso de mecanismos esenciales de provisión.
  - c) Riesgos extraordinarios sobre infraestructuras críticas del ecosistema tokenizado, incluidas sus cadenas de validación, nodos y centros de almacenamiento seguro.
  - d) Situaciones en las que la clasificación de información relativa a reservas pueda generar riesgos de integridad institucional o posibles actos de corrupción.
- 

### **Artículo 23º. Naturaleza de la Información Clasificada y Publicación de Métricas Sintéticas**

Declarase información clasificada, con excepción de los indicadores obligatoriamente públicos previstos en la presente ley, la localización física, rutas logísticas, ubicaciones específicas y condiciones operativas de almacenamiento de las reservas de oro, minerales críticos, combustibles estratégicos y recursos sensibles para la seguridad nacional.

Sin perjuicio de su carácter clasificado, el Poder Ejecutivo deberá garantizar la publicación regular de **métricas agregadas y sintéticas verificables**, que permitan al Congreso y a la ciudadanía evaluar:

- a) La variación porcentual de las reservas estratégicas.
- b) El nivel de presión o deterioro comparado respecto de los umbrales de seguridad.
- c) La situación de riesgo sistémico, conforme a los modelos de alerta establecidos en esta ley.

La omisión injustificada de esta publicación configurará falta grave.

---

### **Artículo 24º. Auditoría Ética sobre Información Clasificada**

La información clasificada vinculada a reservas estratégicas, infraestructura crítica o recursos sometidos a protocolos de seguridad nacional deberá estar siempre sujeta a:

- a) Auditoría criptográfica ciega mediante mecanismos de verificación matemática.
- b) Auditoría ética externa con participación de universidades públicas, organismos multilaterales e integrantes del Registro Ético Nacional.
- c) Auditoría selectiva con el Ministerio de Seguridad y el Ministerio de Defensa para verificar consistencia, integridad y ausencia de riesgos de infiltración o manipulación.

Dichas auditorías deberán garantizar que **ningún dato crítico, aunque sea reservado, quede fuera de trazabilidad.**

---

## **Artículo 25°. Protocolo de Intervención Conjunta ante Riesgo Crítico o Crisis Humanitaria**

En escenarios de crisis extrema definidos por:

- a) Riesgo inminente de hiperinflación o colapso monetario.
- b) Desabastecimiento de alimentos, medicamentos o insumos esenciales.
- c) Amenazas nacionales que comprometan la capacidad del Estado de proteger activos estratégicos.

El Ministerio de Economía, el Ministerio de Seguridad y el Ministerio de Defensa deberán:

1. Activar un **Comando Unificado de Trazabilidad y Resguardo Estratégico**, integrado en tiempo real al sistema de tokenización.
2. Establecer rutas seguras, protocolos blindados y mecanismos especiales de supervisión de activos, movimientos y reservas sensibles.
3. Garantizar la continuidad operativa del ecosistema tokenizado incluso en condiciones de infraestructura degradada, ataques ciberneticos o fallas sistémicas.

La auditoría no accede a identidades, ubicaciones o coordenadas exactas, sino a verificaciones criptográficas.

---

## **Artículo 26°. Redistribución Operativa de Activos y Recursos en Situación de Emergencia**

Durante una emergencia declarada, y previa activación del Comando Unificado, el Estado podrá ejecutar movimientos operativos tokenizados de activos críticos destinados a la protección de la población.

Estos movimientos deberán:

- a) Ser registrados íntegramente en la cadena estatal con verificadores matemáticos.
  - b) Ser accesibles al Congreso y a los órganos de auditoría ética.
  - c) Mantener la reserva de sus detalles físicos o logísticos para no afectar la seguridad nacional.
  - d) Publicar a la ciudadanía un informe sintético que acredite proporcionalidad, destino humanitario y ausencia de desviaciones.
-

## **Artículo 27°. Principio de No Ocultamiento y Control Democrático**

El carácter clasificado de la información no podrá utilizarse para:

- a) Encubrir actos de corrupción.
- b) Ocultar deterioros relevantes de reservas estratégicas.
- c) Eludir auditorías éticas, técnicas o parlamentarias.

Las métricas sintéticas exigidas en esta ley deberán ser siempre públicas, comprensibles y actualizadas en los plazos establecidos, aun durante situaciones de máximo riesgo.

---

## **Artículo 28°. Comunicación al Congreso y a Organismos Internacionales**

Todo evento que implique:

- deterioro abrupto de reservas estratégicas,
- sospecha de apropiación indebida,
- manipulación de información clasificada, o
- riesgo directo para la infraestructura crítica del ecosistema tokenizado,

deberá ser informado en forma inmediata al Congreso de la Nación y a los organismos multilaterales con los que la República mantenga acuerdos de supervisión y cooperación técnica.

---

## **Artículo 29°. Sanciones**

El incumplimiento de los deberes previstos en este capítulo dará lugar a:

- a) suspensión preventiva del funcionario responsable;
- b) apertura obligatoria de auditoría ética extraordinaria;
- c) responsabilidad penal agravada por afectación a la seguridad nacional y al Sistema Ético de Datos Críticos;
- d) nulidad de cualquier acto administrativo que modifique o destruya trazabilidad o métricas críticas.

# **TÍTULO XI — PROCEDIMIENTOS OPERATIVOS PARA EMERGENCIAS,**

# **CRISIS EXTREMAS Y PROTECCIÓN DE ACTIVOS ESTRATÉGICOS**

---

## **Artículo 30°. Activación del Protocolo Nacional de Emergencia Tokenizada (PNET)**

El Protocolo Nacional de Emergencia Tokenizada (PNET) será activado automáticamente ante la verificación de cualquiera de los siguientes supuestos:

- a) Riesgo de hiperinflación o pérdida acelerada del valor real de la moneda.
- b) Interrupción o amenaza grave a la cadena logística o energética nacional.
- c) Ataque cibernético contra nodos o infraestructuras críticas del sistema de tokenización.
- d) Manejo irregular, desviación, pérdida o manipulación de reservas estratégicas.
- e) Crisis humanitaria declarada por el Poder Ejecutivo o por organismos internacionales.
- f) Cualquier amenaza calificada por el Ministerio de Defensa o de Seguridad como riesgo inminente para el patrimonio soberano.

Una vez activado, el PNET tendrá prioridad operativa sobre cualquier protocolo administrativo ordinario.

---

## **Artículo 31°. Niveles de Riesgo y Acciones Obligatorias**

Declaránse los siguientes niveles de riesgo para la toma de decisión:

### **1. Nivel Amarillo – Riesgo Moderado**

Indicadores early-warning detectan tensiones o irregularidades no críticas.

Acciones:

- Auditoría técnica inmediata.
- Refuerzo de verificadores matemáticos.
- Reporte semanal al Ministerio de Economía.

### **2. Nivel Naranja – Riesgo Alto**

Se detectan desvíos relevantes en reservas, trazabilidad o infraestructura.

Acciones:

- Intervención en conjunto con Seguridad y Defensa.
- Activación parcial del Comando Unificado.
- Publicación de métricas sintéticas extraordinarias en un máximo de cinco días.

### **3. Nivel Rojo – Riesgo Crítico o Crisis Humanitaria**

Existe amenaza concreta al patrimonio soberano, al abastecimiento esencial o a la estabilidad institucional.

Acciones obligatorias:

- Activación plena del Comando Unificado.
  - Protección física y digital de reservas estratégicas.
  - Redistribución tokenizada de activos a sectores críticos (salud, energía, alimentos).
  - Publicación urgente de alerta nacional con métricas agregadas verificables.
- 

### **Artículo 32°. Procedimiento de Verificación Criptográfica en Emergencias**

Durante la vigencia del PNET, todos los movimientos de activos estratégicos deberán registrarse en:

- a) Cadenas soberanas de alta seguridad con consenso estatal.
- b) Protocolos de auditoría ciega que permitan validar integridad sin revelar datos clasificados.
- c) Mecanismos anti-manipulación basados en hash encadenados y doble firma pública-institucional.

Es obligación del Estado disponer de **al menos dos copias sincronizadas** del registro:

- una accesible a auditores éticos autorizados,
  - otra aislada en entorno crítico, bajo custodia del Comando Unificado.
- 

### **Artículo 33°. Protocolo de Redistribución Humanitaria de Recursos**

La redistribución extraordinaria de recursos estratégicos en crisis humanitaria deberá cumplir:

- a) Justificación técnica basada en datos tokenizados verificables.
  - b) Registro íntegro del origen, destino y cuantía redistribuida, sin exponer datos logísticos sensibles.
  - c) Dictamen obligatorio de proporcionalidad y urgencia emitido por el Comando Unificado.
  - d) Informe sintético público dentro de los diez días posteriores.
  - e) Prohibición absoluta de beneficiar actores privados sin relevancia social.
-

## **Artículo 34°. Intervención ante Sospecha de Corrupción o Manipulación**

Si durante una emergencia se detectan anomalías, desvíos o intentos de manipulación:

- a) La auditoría ética extraordinaria se activará automáticamente.
  - b) El funcionario o agente involucrado será suspendido preventivamente.
  - c) Se notificará de inmediato a la Justicia Federal con competencia en seguridad y corrupción.
  - d) El sistema generará un bloqueo automático del token afectado para impedir movimientos posteriores.
  - e) El Comando Unificado asegurará físicamente los activos comprometidos.
- 

## **Artículo 35°. Continuidad Operativa en Infraestructura Degradada**

En caso de fallas severas o ataque a la infraestructura tecnológica:

- a) Se activará el Modo Operativo Degradado (MOD), con redundancia en centros soberanos de respaldo.
  - b) Las validaciones se realizarán mediante algoritmos de emergencia con mayor tolerancia a fallos.
  - c) Ningún movimiento estratégico podrá ejecutarse sin doble certificación criptográfica.
  - d) El sistema deberá mantener operatividad mínima para garantizar abastecimiento esencial.
- 

## **Artículo 36°. Protocolo de Comunicación Controlada a la Ciudadanía**

Durante emergencias, la información pública deberá cumplir:

- a) Veracidad verificable.
- b) Mantener reserva de datos clasificados.
- c) Presentar métricas agregadas suficientes para evitar ocultamiento o manipulación.
- d) Evitar generar pánico financiero o social.
- e) Proveer lineamientos claros sobre los pasos a seguir por la población.

Se crea la **Unidad de Comunicación Ética en Emergencias**, coordinada entre Economía, Seguridad, Defensa y Comunicación Pública.

---

## **Artículo 37°. Restablecimiento del Régimen Ordinario**

Finalizada la emergencia, el Estado deberá:

- a) Desactivar el Comando Unificado.
  - b) Emitir un informe completo de todas las operaciones realizadas bajo el PNET.
  - c) Restituir los protocolos de auditoría estándar.
  - d) Garantizar la normalización progresiva de las métricas, indicadores y trazabilidad pública.
  - e) Realizar una auditoría de cierre para evaluar daños, riesgos y aprendizajes.
- 

### **Artículo 38°. Responsabilidad Penal Agravada**

Todo funcionario, agente o entidad que manipule, oculte o distorsione:

- reservas estratégicas,
- indicadores sintéticos,
- auditorías en curso,
- información clasificada,

durante la vigencia del PNET, incurrirá en responsabilidad penal agravada por atentado contra la seguridad nacional, independientemente de su rango o jerarquía.

---

### **Artículo 39°. Reglamentación**

El Poder Ejecutivo reglamentará este capítulo en un plazo máximo de noventa días, estableciendo:

- a) Manuales operativos del PNET.
- b) Capacitación obligatoria anual para funcionarios estratégicos.
- c) Protocolos técnicos de ciberseguridad multicapas.
- d) Límites, excepciones y mecanismos de rendición de cuentas.

## **TITULO XII - INCORPORACIÓN DE ANEXOS TÉCNICOS Y JERARQUÍA NORMATIVA**

### **Artículo 40° — Integración Normativa de los Anexos Técnicos**

Los Anexos Técnicos I a VIII forman parte integrante de la presente Ley y tendrán la misma fuerza jurídica y carácter obligatorio que las disposiciones contenidas en el cuerpo normativo principal.

Dichos anexos poseen carácter operativo, técnico, metodológico y procedimental, y serán de aplicación directa en todos los organismos alcanzados por esta Ley.

---

### **Artículo 41° — Actualización Dinámica de Anexos**

Los Anexos Técnicos podrán ser actualizados por la Autoridad Nacional de Tokenización Ética, previa:

- a) Auditoría ética externa;
- b) Dictamen técnico de universidades nacionales;
- c) Comunicación formal a la Comisión Bicameral del Congreso;
- d) Publicación en el Boletín Oficial.

Las actualizaciones no podrán modificar el espíritu, objeto o finalidad de la Ley, sino únicamente adaptar parámetros, metodologías, matrices, algoritmos y procedimientos técnicos a nuevas necesidades o riesgos emergentes.

---

### **Artículo 42° — Carácter Vinculante y Obligatorio de los Anexos**

Las normas contenidas en los Anexos Técnicos serán vinculantes para:

- a) todos los organismos de la Administración Pública Nacional;
- b) empresas públicas y mixtas;
- c) operadores autorizados del Ecosistema Nacional de Tokenización Ética;
- d) nodos del Sistema de Infraestructura Crítica;
- e) proveedores tecnológicos sujetos a soberanía tecnológica.

El incumplimiento de los parámetros obligatorios de los Anexos será considerado infracción grave.

---

### **Artículo 43° — Alcance de los Anexos Técnicos**

Los Anexos comprenderán, con carácter no taxativo:

1. **Matriz de Clasificación de Información para Tokenización**
2. **Indicadores Sintéticos y Métricas Públicas sobre Reservas Estratégicas**
3. **Modelos de Tableros de Control y Paneles Ciudadanos**
4. **Modelo de Tipología de Tokens Soberanos**
5. **Protocolo Nacional de Auditoría Ética**
6. **Algoritmo de Detección Temprana de Riesgo Sistémico**
7. **Procedimiento Técnico de Activación del PNET en Emergencias**

## **8. Matriz de Decisión para Redistribución Humanitaria de Activos**

Cada uno de estos anexos será de implementación obligatoria y complementaria a los artículos de la presente Ley.

---

### **Artículo 44° — Control Parlamentario**

La Comisión Bicameral Permanente tendrá competencia para:

- a) supervisar el cumplimiento de los Anexos Técnicos;
  - b) requerir auditorías extraordinarias cuando surjan inconsistencias o alertas;
  - c) solicitar modificaciones o actualización de anexos;
  - d) emitir recomendaciones vinculantes para la Autoridad de Aplicación.
- 

### **Artículo 45° — Articulación con el PNED**

En caso de activación del Protocolo Nacional de Emergencia Tokenizada:

- a) serán obligatorios los Anexos VII y VIII;
  - b) los mecanismos del Anexo VI tendrán prioridad operativa sobre sistemas ordinarios;
  - c) las métricas e indicadores del Anexo II deberán publicarse con la frecuencia excepcional prevista en esta Ley;
  - d) los tableros públicos del Anexo III deberán actualizarse mediante parámetros de emergencia.
- 

### **Artículo 46° — Aplicación Subsidiaria**

En caso de vacío interpretativo o ausencia de procedimiento explícito, los Anexos Técnicos se aplicarán de manera subsidiaria, prevaleciendo:

1. la protección de la soberanía nacional;
  2. la integridad de activos estratégicos;
  3. la trazabilidad ética verificable;
  4. la prevención del riesgo sistémico.
- 

### **Artículo 47° — Reglamentación**

El Poder Ejecutivo reglamentará este Título dentro de un plazo máximo de **60 días**, estableciendo:

- a) mecanismos de actualización técnica;
- b) ciclos de auditoría sobre el uso de los Anexos;
- c) estándares mínimos para interoperabilidad;
- d) lineamientos obligatorios de publicación.

#### **Artículo 48° — Renegociación Soberana de Recursos Estratégicos, Reservas y Tecnologías Asociadas mediante Tokenización Ética**

El Estado Nacional, en el marco de la presente Ley, tendrá la facultad y obligación de **renegociar, revisar, auditar y modificar** contratos, concesiones, acuerdos tecnológicos, infraestructuras críticas instaladas y cualquier sistema asociado a la gestión de **recursos estratégicos, reservas naturales, infraestructuras SCADA, telemetría, datos sensibles o activos de alto valor soberano**, cuando se verifique cualquiera de las siguientes condiciones:

- a) existencia de riesgos para la soberanía tecnológica,
- b) vulneración de la integridad de los datos o reservas,
- c) dependencia operativa o tecnológica no razonable,
- d) incumplimientos contractuales técnicos o de seguridad,
- e) riesgo geopolítico, cibernético o ambiental,
- f) afectación a la continuidad operacional o a la autonomía estatal.

---

#### **1. Auditoría Técnica y Jurídica Obligatoria para la Renegociación**

El Estado efectuará auditoría técnica inmediata, con carácter previo a la renegociación, que abarcará:

1. Acceso pleno a datos de sensores, SCADA, telemetría y sistemas asociados.
2. Acceso obligatorio a:
  - planos técnicos,
  - arquitectura de red,
  - firmware, software y drivers instalados,
  - logs de operación,
  - manuales,
  - credenciales maestras.
3. Identificación de:
  - dependencias ocultas,
  - servidores externos,
  - almacenamiento en el extranjero,
  - puertas traseras o accesos administrativos,
  - telemetría exportada,
  - licencias restrictivas,
  - monopolios tecnológicos sin repuestos.

Los hallazgos de auditoría serán causa suficiente para renegociar, corregir, modificar, suspender o exigir anexos complementarios.

---

## 2. Renegociación Progresiva mediante Anexos Complementarios

Aun cuando el contrato original se encuentre vigente, el Estado podrá exigir **Anexos Complementarios Soberanos**, sin alterar la validez del contrato principal, mediante los cuales se establezca:

- a) soberanía de datos y almacenamiento local obligatorio en infraestructura nacional,
- b) interoperabilidad obligatoria con sistemas soberanos,
- c) retiro de software de telemetría externa,
- d) entrega completa de manuales, documentación y firmware,
- e) provisión de credenciales maestras para acceso estatal,
- f) protocolos propios de emergencia y continuidad operacional,
- g) auditorías técnicas y criptográficas recurrentes,
- h) cumplimiento obligatorio de la Ley de Tokenización Ética.

Los anexos complementarios serán de cumplimiento obligatorio para los proveedores y se entenderán integrados a la relación contractual existente.

---

## 3. Independencia Técnica Progresiva

El Estado desarrollará, directamente o mediante universidades, CONICET u organismos técnicos, las capacidades para:

- a) operar, mantener y auditar las infraestructuras instaladas sin depender del proveedor,
- b) replicar componentes funcionales mediante software libre o estándares abiertos,
- c) construir un **gemelo digital soberano** para el análisis local y la planificación,
- d) documentar integralmente la infraestructura para asegurar autonomía futura.

Cuando la independencia técnica sea alcanzada, el Estado podrá prescindir de servicios del proveedor sin penalidad.

---

## 4. Reversión de Riesgos para la Soberanía

Toda renegociación deberá priorizar la reversión de riesgos en:

### **a) Datos**

- replicación local completa,
- prohibición de control extranjero sobre datos críticos,
- aislamiento de redes sensibles,
- prohibición de exportar telemetría.

### **b) Infraestructura Crítica**

- eliminación progresiva de componentes propietarios no auditables,
- inventario nacional de repuestos, firmware y drivers,
- verificación de continuidad operacional sin proveedores externos.

### **c) Jurisdicción**

- revisión de cláusulas de arbitraje internacional,
  - renegociación de cláusulas leoninas,
  - anulación de disposiciones que afecten la soberanía o seguridad nacional.
- 

## **5. Congelamiento de Nuevas Concesiones hasta Garantizar Soberanía Plena**

Hasta tanto la infraestructura existente cumpla con los estándares de esta Ley, queda prohibida la incorporación de:

- a) nuevas obras,
- b) ampliaciones,
- c) integraciones tecnológicas,
- d) servicios adicionales,
- e) actualizaciones de software o hardware,

que impliquen:

- dependencia tecnológica no razonable,
- telemetría externa,
- pérdida de soberanía de datos,
- uso de infraestructura extranjera no auditada,
- incumplimiento del régimen de tokenización ética.

Toda nueva concesión deberá incluir desde el inicio cláusulas de soberanía tecnológica, auditoría continua, interoperabilidad soberana y tokenización ética obligatoria.

---

## **6. Prioridad Normativa**

La renegociación soberana basada en este artículo prevalecerá sobre cualquier cláusula contractual previa que:

- a) limite la auditoría estatal;
- b) impida el acceso a documentación esencial;
- c) restrinja el acceso a código, firmware o telemetría;
- d) otorgue control exclusivo al proveedor;
- e) delegue jurisdicción en tribunales extranjeros cuando afecte infraestructura estratégica.

Toda cláusula contraria a este artículo será nula de nulidad absoluta.

---

## **7. Publicación y Control**

El Estado deberá publicar mensualmente un **Reporte de Renegociación Soberana**, con:

- estado de auditorías,
- avances en independencia técnica,
- vulnerabilidades corregidas,
- anexos complementarios firmados,
- retrocesos o incumplimientos del proveedor,
- grado de soberanía alcanzado.

Los datos sensibles se presentarán en forma sintética, conforme a esta Ley.

# **TÍTULO XIII — INTERVENCIÓN DE ORGANISMOS NEUTRALES INTERNACIONALES EN PROCESOS DE RENEGOCIACIÓN SOBERANA**

---

**Artículo 49° — Supuestos que habilitan la intervención internacional neutral**

El Estado Nacional podrá requerir la intervención de organismos internacionales neutrales, técnicos y no injerencistas, cuando se verifique alguno de los siguientes supuestos:

- a) presunta afectación de la soberanía tecnológica o de datos estratégicos;
  - b) falta de acceso estatal a contratos completos, anexos o documentación técnica;
  - c) dudas fundadas sobre el impacto ambiental, operativo o de seguridad;
  - d) sospecha de dependencia tecnológica indebida;
  - e) opacidad en transferencias tecnológicas o concesiones sobre recursos estratégicos;
  - f) riesgo geopolítico derivado del manejo extranjero de información crítica.
- 

## **Artículo 50° — Facultades de los organismos neutrales internacionales**

Los organismos neutrales internacionales convocados podrán:

1. **Revisar si la transferencia tecnológica violó la soberanía nacional**, la integridad territorial o los criterios de seguridad establecidos por esta Ley.
  2. **Requerir acceso a los contratos completos**, incluidos anexos, cláusulas reservadas, acuerdos accesorios y documentación técnica vinculada, aun cuando existan restricciones de divulgación interna.
  3. **Ordenar auditorías técnicas, ambientales, criptográficas y de seguridad**, cuando la complejidad o sensibilidad de la infraestructura lo requiera.
  4. **Evaluar el riesgo geopolítico derivado del control, almacenamiento o uso extranjero de datos asociados a recursos estratégicos, cuencas hídricas, infraestructura energética o territorios críticos.**
  5. **Recomendar la renegociación total o parcial del acuerdo**, o la limitación de cláusulas contrarias a esta Ley.
  6. **Exigir la repatriación de datos, firmware, modelos predictivos, logs y algoritmos**, cuando se encuentren alojados o controlados en jurisdicciones extranjeras.
  7. **Sugerir marcos normativos de tokenización ética para recursos naturales**, conforme a estándares internacionales de seguridad y sostenibilidad.
  8. **Detectar indicios de irregularidades, conflictos de intereses o incompatibilidades éticas** en la negociación o ejecución del acuerdo.
  9. **Proponer la suspensión, rescisión o nulidad parcial**, si se verifican perjuicios para el Estado.
- 

## **Artículo 51° — Carácter vinculante de los informes internacionales**

Los informes emitidos por los organismos internacionales neutrales tendrán:

- 
- a) carácter técnico vinculante en materia de seguridad, soberanía de datos y auditoría;
  - b) carácter recomendatorio en materia política, operativa o comercial;
  - c) prioridad sobre cualquier cláusula contractual previa que afecte la soberanía nacional, la seguridad de datos o el interés estratégico del Estado.
- 

## **Artículo 52° — Procedimiento para la solicitud de intervención internacional**

La intervención podrá ser solicitada por:

- a) la Autoridad Nacional de Tokenización Ética;
- b) el Poder Ejecutivo;
- c) la Comisión Bicameral de Seguimiento;
- d) gobernadores o entidades federales cuando existan recursos estratégicos provinciales involucrados.

La solicitud deberá fundamentarse técnicamente y acompañarse de antecedentes, informes preliminares y documentación disponible.

---

## **Artículo 53° — Garantías de independencia y neutralidad**

Los organismos convocados deberán:

- a) ser técnicamente competentes y no vinculados a Estados o empresas con intereses en la infraestructura evaluada;
  - b) contar con reconocimiento internacional en auditoría técnica, ambiental, o de seguridad cibernética;
  - c) trabajar bajo estándares de neutralidad, transparencia y confidencialidad reforzada;
  - d) realizar sus evaluaciones en territorio nacional, salvo casos excepcionales debidamente justificados.
- 

## **Artículo 54° — Obligación de acceso pleno**

Toda empresa, entidad o proveedor involucrado en la transferencia tecnológica auditada estará obligado a:

- a) facilitar el acceso completo a documentación técnica, operativa, comercial y contractual;
- b) habilitar auditorías presenciales en instalaciones críticas;
- c) entregar copias integrales de firmware, software, logs y configuraciones;

- d) permitir análisis forense de redes, SCADA y sistemas de telemetría;
- e) remover cualquier obstáculo operativo o jurídico que impida la revisión internacional.

El incumplimiento será considerado **infracción gravísima** y causal de rescisión inmediata.

---

### **Artículo 55° — Publicación y transparencia**

El informe final emitido por el organismo internacional deberá:

- a) publicarse en forma sintética para la ciudadanía;
  - b) resguardar información clasificada conforme la Ley;
  - c) incluir el grado de riesgo, dependencia, impacto ambiental y soberanía comprometida;
  - d) detallar recomendaciones de renegociación o rescisión.
- 

### **Artículo 56° — Articulación con el Protocolo Nacional de Emergencia Tokenizada (PNET)**

Si la auditoría internacional detecta un riesgo grave o crítico:

- a) la Autoridad de Aplicación podrá activar el PNET en forma preventiva;
  - b) el Estado podrá suspender temporalmente la operación del sistema auditado;
  - c) los organismos internacionales podrán colaborar en la mitigación del riesgo;
  - d) los datos necesarios para la emergencia deberán repatriarse de inmediato.
- 

### **Artículo 57° — Responsabilidad Internacional del Proveedor**

Si los organismos neutrales detectan:

- a) ocultamiento deliberado,
- b) exportación no autorizada de datos,
- c) manipulación tecnológica,
- d) puertas traseras,
- e) telemetría desautorizada,
- f) incumplimientos ambientales o de continuidad,

el proveedor será responsable:

1. administrativa y civil,
2. penal en caso de afectar la seguridad nacional,

3. internacionalmente según corresponda,
4. obligado a reparar económicamente los daños ocasionados.

## TÍTULO XIV — AUDITORÍA ESTRATÉGICA SOBRE RECURSOS CRÍTICOS Y ARTICULACIÓN CON DEFENSA NACIONAL

---

### Artículo 58° — Recursos Estratégicos como Activos de Seguridad Nacional

Los recursos naturales estratégicos, reservas críticas, infraestructuras de monitoreo, sistemas SCADA, datos de cuencas, redes logísticas y cualquier infraestructura asociada a su explotación o seguimiento serán considerados **activos de seguridad nacional** a los efectos de esta Ley.

La pérdida de control técnico, informativo o algorítmico sobre dichos activos será considerada riesgo estratégico grave.

Los activos estratégicos tokenizados se consideran de interés esencial para la defensa nacional, conforme estándares de seguridad del Estado argentino

---

### Artículo 59° — Competencia Conjunta con el Sistema de Defensa

La auditoría técnica, ambiental, algorítmica y de soberanía de datos sobre recursos estratégicos será realizada:

- a) por la Autoridad Nacional de Tokenización Ética,
- b) con participación obligatoria del Ministerio de Defensa,
- c) y asesoramiento de los Estados Mayores Conjuntos cuando la infraestructura auditada impacte:
  - rutas logísticas críticas,
  - cuencas hídricas estratégicas,
  - sistemas energéticos,
  - fronteras inteligentes,
  - vigilancia del territorio,
  - ciberdefensa militar.

---

## **Artículo 60° — Ciberdefensa y Auditoría Crítica Conjunta**

Toda auditoría que detecte vulnerabilidades tecnológicas, telemetría externa, acceso extranjero a infraestructura crítica o riesgos geopolíticos deberá ser comunicada de forma inmediata al **Comando Conjunto de Ciberdefensa**, el cual podrá:

- a) intervenir redes y sistemas para aislamiento,
  - b) ordenar medidas preventivas en infraestructura crítica,
  - c) coordinar con inteligencia militar,
  - d) activar protocolos de defensa cibernética.
- 

## **Artículo 61° — Acceso irrestricto del Estado a datos y firmware en infraestructura estratégica**

Todo operador o proveedor, nacional o extranjero, deberá garantizar:

- a) acceso total al firmware,
- b) acceso a telemetría local,
- c) acceso a logs y modelos predictivos,
- d) acceso a arquitecturas de red,
- e) entrega de credenciales maestras.

La negativa será considerada amenaza a la seguridad nacional y causal de rescisión inmediata.

---

## **Artículo 62° — Intervención de organismos internacionales neutrales en casos de riesgo estratégico**

Cuando se presuma afectación de la soberanía en infraestructura estratégica, el Estado podrá convocar organismos internacionales neutrales para:

1. verificar vulneraciones a la soberanía,
2. revisar contratos ocultos,
3. auditar infraestructura crítica,
4. evaluar riesgo geopolítico,
5. sugerir renegociación o rescisión,
6. exigir repatriación de datos,
7. detectar conflictos de intereses,
8. emitir dictámenes sobre seguridad estratégica.

Sus informes tendrán carácter vinculante en materia de seguridad de datos y continuidad operacional.

---

### **Artículo 63° — Integración con la Defensa Territorial**

Los resultados de auditoría serán integrados como insumos para:

- a) inteligencia estratégica,
  - b) planificación militar,
  - c) análisis de riesgos territoriales,
  - d) geopolítica hídrica, energética y ambiental,
  - e) defensa de infraestructuras críticas.
- 

### **Artículo 64° — Emergencias y control estatal directo**

Ante detección de riesgo crítico o grave que involucre infraestructura estratégica:

- a) el Estado podrá tomar control operacional directo,
  - b) aislar redes,
  - c) suspender concesiones,
  - d) tomar posesión temporal de tecnología o activos,
  - e) activar el PNET,
  - f) disponer intervención militar en ciberdefensa.
- 

### **Artículo 65° — Prohibición de cesión de datos estratégicos a jurisdicciones extranjeras**

Queda prohibida toda transferencia, copia, exportación, visualización, almacenamiento o análisis en servidores extranjeros de:

- datos de cuencas hídricas,
- litio y minerales críticos,
- reservas energéticas,
- infraestructura crítica,
- sistemas logísticos o fronterizos.

Cualquier violación será considerada delito de seguridad nacional.

---

## **Artículo 66° — Renegociación reforzada para infraestructura estratégica**

La renegociación de contratos sobre recursos estratégicos deberá incluir:

- a) repatriación de datos,
  - b) retiro de telemetría externa,
  - c) soberanía de firmware,
  - d) auditoría continua,
  - e) interoperabilidad soberana,
  - f) cláusulas de defensa nacional,
  - g) dominio operativo estatal 24/7,
  - h) prohibición de puertas traseras.
- 

## **Artículo 67° — Control parlamentario especializado**

La Comisión Bicameral de Seguridad, Defensa y Recursos Estratégicos supervisará:

- los informes de auditoría,
- la intervención internacional,
- la renegociación de infraestructura estratégica,
- la ejecución de medidas de defensa digital.

# **TÍTULO XV — CONTINUIDAD OPERATIVA DEL ESTADO Y PROTECCIÓN DE LA POBLACIÓN EN ESCENARIOS DE CRISIS EXTREMA**

---

## **Artículo 68° — Principio de Continuidad Operativa del Estado**

La presente Ley reconoce la **continuidad operativa del Estado** como un principio superior de interés público.

Durante escenarios de riesgo extremo —incluyendo hiperinflación, crisis humanitaria, desabastecimiento, fallas sistémicas o pérdida de capacidad estatal— el Estado deberá asegurar el funcionamiento mínimo indispensable de los sistemas que sostienen la vida, integridad y seguridad de la población.

---

## **Artículo 69° — Alcance Operativo**

A los efectos de esta Ley, se consideran servicios críticos para la continuidad del Estado:

- a) energía (producción, transporte, distribución),
  - b) agua y cuencas hídricas,
  - c) combustibles,
  - d) logística de alimentos,
  - e) infraestructura de comunicaciones,
  - f) sensores, SCADA y telemetría del territorio,
  - g) reservas estratégicas,
  - h) minería crítica (litio, cobre, uranio),
  - i) redes de transporte esenciales,
  - j) infraestructura de salud y emergencias.
- 

## **Artículo 70° — Auditoría Estratégica para Crisis Humanitaria**

Ante riesgo extremo, la Autoridad Nacional de Tokenización Ética realizará **auditoría inmediata**, con participación de:

- Ministerio de Defensa,
- Comando Conjunto de Ciberdefensa,
- Ministerio de Seguridad,
- provincias afectadas.

La auditoría deberá determinar:

1. riesgos de interrupción de servicios esenciales,
  2. dependencia tecnológica extranjera,
  3. telemetría externa no autorizada,
  4. posible pérdida de control estatal sobre recursos críticos,
  5. fallas que puedan agravar la crisis humanitaria.
- 

## **Artículo 71° — Acceso Estatal Garantizado a Infraestructura Crítica**

Durante emergencias, el Estado tendrá derecho a acceso inmediato a:

- firmware,
- credenciales maestras,
- logs operativos,

- datos en tiempo real,
- algoritmos de predicción,
- modelos matemáticos de demanda y oferta,
- servidores, paneles y tableros operativos.

Toda negativa será considerada **amenaza directa a la seguridad nacional** y causal de intervención.

---

### **Artículo 72° — Control Estatal Directo en Caso de Riesgo Grave**

Cuando la auditoría determine riesgo crítico de:

- apagón informativo,
- interrupción de servicios esenciales,
- fuga de datos estratégicos,
- abandono de obligaciones del proveedor,
- riesgo para la vida o integridad de la población,

el Estado podrá asumir **control temporal directo** de la infraestructura, mediante:

- a) intervención operativa civil,
  - b) soporte de ciberdefensa militar,
  - c) aislamiento de redes,
  - d) suspensión de concesiones,
  - e) administración técnica estatal hasta restituir la normalidad.
- 

### **Artículo 73° — Intervención Internacional Neutral en Crisis Estratégicas**

Si el riesgo involucra infraestructura extranjera o contratos lesivos, el Estado podrá solicitar **auditoría internacional neutral** con competencias para:

- verificar violaciones a la soberanía,
- ordenar repatriación de datos,
- recomendar renegociación o rescisión,
- validar jurídicamente la intervención estatal en emergencia.

Sus dictámenes serán vinculantes en materia de seguridad operativa.

---

### **Artículo 74° — Publicación de Indicadores Críticos en Emergencia**

El Estado deberá publicar, durante la emergencia, indicadores sintéticos no confidenciales sobre:

- disponibilidad energética,
  - reservas de agua segura,
  - estado de la logística esencial,
  - fallas operativas detectadas,
  - medidas correctivas adoptadas.
- 

#### **Artículo 75° — Protección de la Población como Finalidad Prioritaria**

Todas las acciones previstas en este Título se interpretarán con un único objetivo: **garantizar la protección de la población y la continuidad operativa del país**, incluso cuando circunstancias económicas, financieras o geopolíticas pongan en riesgo la capacidad estatal.

---

#### **Artículo 76° — Prevalencia Normativa**

Las facultades previstas en este Título prevalecerán sobre cláusulas contractuales, concesiones, delegaciones o acuerdos que impidan la continuidad operativa del Estado o pongan en riesgo la vida o la seguridad de la población.

## **TITULO XVI – GOBERNANZA ETICA DE SISTEMAS ALGORITMICOS E INTELIGENCIA ARTIFICIAL**

### **Artículo 77° – Prevención de arquitecturas monetarias privadas con riesgo sistémico y estándar de interoperabilidad soberana**

#### **1. Prohibición de sistemas monetarios cerrados de escala global:**

Queda expresamente prohibida la implementación, promoción o despliegue en territorio nacional de infraestructuras digitales, criptomonedas, stablecoins, tokens de valor o sistemas de pagos que, bajo control privado o paraestatal, pretendan operar como **moneda paralela, infraestructura de compensación transnacional o red financiera soberana** sin supervisión democrática directa. Se consideran de alto riesgo aquellos modelos equivalentes al proyecto **LIBRA/DIEM de Meta (Facebook)** debido a su capacidad para:  
a) capturar usuarios por red global;

- b) desintermediar bancos centrales;
  - c) generar dependencia tecnológica en infraestructura de custodia y gobernanza;
  - d) erosionar la política monetaria nacional.
- 2. Principio de Soberanía Digital Económica:**
- Toda infraestructura de tokenización, stablecoin pública, sistema de pagos tokenizado o red de activos digitales deberá operar bajo **jurisdicción nacional y gobernanza auditada**, garantizando:
- a) control público sobre reservas, algoritmos, validadores, cambios de protocolo y estabilidad;
  - b) independencia respecto de corporaciones tecnológicas extranjeras;
  - c) imposibilidad de que un ente privado acumule el poder para emitir, congelar o manipular activos equivalentes a moneda de curso no oficial.
- 3. Obligación de Interoperabilidad Ética y Transparente:**
- Ningún token, red o plataforma podrá operar en esquemas cerrados (“walled garden”) que impidan supervisión, migración o auditoría.
- Se exige:
- a) estándares abiertos de criptografía, gobernanza y trazabilidad;
  - b) interoperabilidad regulatoria con sistemas estatales;
  - c) arquitectura pública para auditoría en tiempo real;
  - d) garantías contra modelos de “reserva sintética” opacos como los previstos en LIBRA.
- 4. Evaluación de Riesgo Macrofinanciero Obligatoria (ERMO):**
- Todo proyecto de tokenización con impacto monetario deberá presentar una ERMO que determine:
- a) exposición sistémica;
  - b) riesgo de dolarización indirecta o competencia desleal con la moneda nacional;
  - c) potencial concentración de poder algorítmico;
  - d) riesgos de fuga de capitales digital automatizada;
  - e) riesgos derivados de gobernanza privada de alto volumen (caso Meta–Calibra).
- 5. Prohibición de gobernanza algorítmica no democrática:**
- Se prohíben los modelos en los que una corporación o consorcio pueda controlar:
- a) políticas de emisión;
  - b) estabilidad o devaluación del token;
  - c) listas negras de usuarios;
  - d) criterios automáticos de bloqueo o censura financiera.
- Estos riesgos fueron documentados en el proyecto LIBRA, que permitía a Meta actuar como banco central paralelo.
- 6. Requisito de Supervisión Continua Multisectorial:**
- Toda infraestructura debe estar bajo vigilancia conjunta del Estado, organismos de control, ciudadanía experta y auditorías independientes.
- Ningún sistema podrá operar con cláusulas de arbitraje internacional para evadir responsabilidades (uno de los riesgos señalados en el diseño de LIBRA).
- 7. Cláusula de Protección Social y de Derechos Humanos:**
- Se prohíbe cualquier mecanismo que pueda derivar en manipulación económica masiva, vigilancia financiera, discriminación algorítmica o condicionamiento de

beneficios sociales mediante redes privadas tipo LIBRA. La infraestructura de tokenización ética es un **bien público**, no un negocio corporativo.

## **TITULO XVII - TRANSFERENCIA TECNOLÓGICA, AUDITORÍA SOBERANA Y RENEGOCIACIÓN ÉTICA EN SISTEMAS CRÍTICOS**

**Artículo 78° — Principio de soberanía tecnológica y de datos.** Toda transferencia tecnológica, provisión de sistemas digitales, infraestructura inteligente, plataformas de gestión, sensores, sistemas SCADA, algoritmos, modelos predictivos o soluciones basadas en datos vinculadas a recursos naturales, servicios públicos esenciales o infraestructuras críticas deberá ajustarse al principio de soberanía tecnológica, soberanía de datos y control público efectivo, aun cuando los contratos hubieran sido celebrados con anterioridad a la entrada en vigencia de la presente ley.

**Artículo 79° — Derecho irrenunciable a la auditoría técnica y jurídica.** El Estado Nacional, las provincias y los municipios conservan en todo momento el derecho irrenunciable a realizar auditorías técnicas, jurídicas, financieras, ambientales y de ciberseguridad sobre cualquier sistema tecnológico aplicado a recursos estratégicos o servicios esenciales, aun cuando la tecnología ya se encuentre instalada y operativa.

Dicho derecho comprende, como mínimo, el acceso a datos, arquitectura de red, software, firmware, manuales, logs operativos y credenciales necesarias para auditoría. La negativa injustificada constituirá incumplimiento grave.

**Artículo 80° — Auditoría como causal de renegociación.** La detección de dependencias tecnológicas ocultas, almacenamiento de datos fuera del territorio nacional, accesos remotos no controlados, licencias restrictivas, monopolios técnicos o riesgos a la soberanía habilitará la renegociación parcial del contrato mediante anexos técnicos o jurídicos.

**Artículo 81° — Renegociación progresiva mediante acuerdos complementarios.** El Estado podrá exigir acuerdos complementarios obligatorios en materia de soberanía de datos, interoperabilidad, ciberseguridad, protocolos de emergencia, capacitación y acceso administrativo, sin que ello implique rescisión automática del contrato principal.

**Artículo 82° — Repatriación y control de datos estratégicos.** Toda información generada mediante sistemas tecnológicos aplicados a recursos estratégicos deberá contar con copia íntegra y operativa en servidores bajo jurisdicción nacional o provincial, quedando prohibido el control exclusivo por entidades extranjeras.

**Artículo 83° — Adquisición de independencia técnica.** La autoridad competente deberá implementar planes de independencia técnica que incluyan formación de personal, documentación completa, replicación funcional y desarrollo de gemelos digitales de control público.

**Artículo 84° — Limitaciones a la jurisdicción extranjera.** Serán revisables o nulas las cláusulas que impongan arbitraje extranjero obligatorio, restrinjan auditorías o comprometan la continuidad operativa de servicios esenciales.

**Artículo 85° — Congelamiento soberano de expansiones futuras.** Toda ampliación o actualización tecnológica deberá ajustarse plenamente a los principios de la presente ley, aun cuando el contrato original no los hubiera contemplado.

**Artículo 14° — Tokenización ética como instrumento de control.** La tokenización ética deberá utilizarse como herramienta de auditoría permanente, trazabilidad y prevención de dependencias tecnológicas, quedando prohibidos los esquemas opacos o inaccesibles para la autoridad pública.

**Artículo 86° — Autoridad de coordinación interinstitucional.** Créase la Unidad Interinstitucional de Auditoría y Soberanía Tecnológica como órgano de coordinación de auditorías integrales y políticas de tokenización ética en sistemas críticos.

## TITULO XVIII - DISPOSICIONES TRANSITORIAS Y FINALES

**Artículo 87° — Adecuación.** Las disposiciones de la presente ley son de orden público y de aplicación inmediata cuando se encuentren comprometidos la soberanía, la seguridad o los derechos colectivos. Los organismos estatales deberán adecuar sus sistemas en un plazo máximo de doce meses.

**Artículo 88° — Reglamentación.**

El Poder Ejecutivo reglamentará la presente Ley dentro de los noventa días de su promulgación.

**Artículo 89° — Vigencia.**

La Ley entra en vigencia el día de su publicación.

# **FUNDAMENTOS**

Considerando:

Que los recursos naturales estratégicos, las reservas críticas, las infraestructuras esenciales, los sistemas de control territorial, los sensores, la telemetría, los SCADA, los datos operativos y los algoritmos predictivos constituyen hoy los pilares que sostienen el funcionamiento del país, la seguridad nacional y el bienestar de la población.

Que la ausencia de marcos normativos modernos ha generado vulnerabilidades, dependencias tecnológicas, pérdida de trazabilidad, riesgos de fuga de información estratégica, y limitaciones operativas que pueden agravarse en escenarios de crisis como hiperinflación, desabastecimiento o emergencias humanitarias.

Que la Argentina debe contar con herramientas jurídicas que garanticen transparencia, auditoría ética, control estatal, soberanía de datos, repatriación de información crítica, independencia tecnológica, continuidad operativa del Estado y protección efectiva de la población ante riesgos sistémicos.

Que la tokenización ética —en tanto mecanismo de representación verificable, auditible y segura de activos, procesos y datos críticos— ofrece una vía concreta para fortalecer la gobernanza, la trazabilidad pública no riesgosa, la protección de infraestructuras críticas, la auditoría ciudadana y la defensa integral del territorio y los recursos del país.

Que la presente iniciativa surge desde la sociedad civil, con el propósito de aportar una arquitectura normativa moderna, sólida y compatible con estándares internacionales, para prevenir vulnerabilidades, recuperar capacidad operativa, garantizar soberanía tecnológica y consolidar un modelo de desarrollo estratégico basado en ética, seguridad y transparencia.

En virtud de lo expuesto, y en pleno ejercicio del derecho ciudadano a proponer normas para la protección del interés público, la seguridad nacional y la continuidad operativa del país, se presenta el siguiente:

**PROYECTO DE LEY DE TOKENIZACIÓN ÉTICA, SOBERANÍA TECNOLÓGICA Y PROTECCIÓN DE RECURSOS ESTRATÉGICOS DE ARGENTINA.**

La presente ley tiene como finalidad establecer un marco normativo integral frente a los crecientes procesos de digitalización, tokenización y transferencia tecnológica aplicados a recursos naturales, infraestructuras críticas y servicios públicos esenciales.

La experiencia reciente demuestra que numerosos contratos tecnológicos celebrados sin estándares de soberanía han generado dependencias estructurales, pérdida de control sobre datos estratégicos, opacidad contractual y vulnerabilidades en materia de seguridad, ambiente y derechos humanos.

La tokenización ética se propone como una herramienta de trazabilidad y control público, no como un mecanismo de privatización encubierta. Asimismo, la ley reconoce el derecho irrenunciable del Estado a auditar, renegociar y corregir contratos tecnológicos aun cuando estos se encuentren en ejecución, cuando esté en juego el interés público.

El presente proyecto se apoya en la Constitución Nacional, en particular en los artículos vinculados al dominio originario de los recursos naturales por parte de las provincias, la protección de los derechos colectivos y el deber indelegable del Estado de garantizar servicios esenciales.

Por todo lo expuesto, se solicita la aprobación del presente proyecto de ley.

### **Antecedentes y experiencias internacionales en tokenización ética**

La presente iniciativa no constituye una innovación aislada ni una creación desvinculada de los estándares globales vigentes. Por el contrario, se inscribe en un conjunto de experiencias internacionales que utilizan tecnologías de tokenización y registros distribuidos con fines éticos, ambientales, científicos y sociales, alineadas con los lineamientos de Naciones Unidas, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Unión Internacional de Telecomunicaciones (UIT).

En materia ambiental y energética, proyectos como **Chia Network** (Estados Unidos) y **Toucan Protocol** (Europa y América Latina) han implementado sistemas de tokenización de créditos de carbono verificados, permitiendo trazabilidad pública, auditoría del impacto ambiental y reducción de intermediaciones opacas. Estas experiencias demuestran que la tokenización puede utilizarse como herramienta de control, transparencia y sostenibilidad, y no únicamente con fines especulativos.

En el ámbito del conocimiento y los bienes comunes digitales, iniciativas como **Ocean Protocol** y desarrollos promovidos por **UNESCO Labs** han avanzado en la tokenización ética de datos científicos y producción intelectual, garantizando protección de la autoría, licencias de uso responsable y distribución equitativa del valor generado. Estos modelos resultan particularmente relevantes para sistemas científicos públicos y universidades.

Asimismo, en el sector productivo y de economía circular, plataformas como **Circularise** en la Unión Europea utilizan tecnologías de registro distribuido para asegurar la trazabilidad de materiales reciclados, fortaleciendo cadenas de valor locales, reduciendo fraudes y promoviendo prácticas industriales sostenibles.

En el plano de la participación ciudadana, diversos Estados han experimentado mecanismos de identidad y participación digital basados en tokens no monetarios, orientados a validar procesos de gobernanza abierta y fortalecer la confianza pública, sin mercantilizar la identidad ni vulnerar derechos fundamentales.

Cabe señalar, asimismo, que la experiencia internacional también ha evidenciado usos no éticos de la tokenización, como en el caso de proyectos que intentan financiarizar datos biométricos sensibles. Estos antecedentes refuerzan la necesidad de establecer marcos normativos claros que prohíban prácticas extractivas de datos personales y garanticen soberanía, control ciudadano y protección de derechos.

En este contexto, la Ley de Tokenización Ética propuesta adapta dichas experiencias al marco constitucional argentino, orientando la tokenización hacia fines de auditoría pública, trazabilidad responsable, soberanía tecnológica, protección de recursos estratégicos y fortalecimiento del Estado, evitando expresamente su utilización especulativa o contraria al interés público.

**Firmado:**

**Natividad Vidal**

Autora del Proyecto

Capilla del Monte, Córdoba, Argentina

**Firma manuscrita digital:**



Natividad Vidal

DNI 27.716.481

**Correo institucional:**

datosabiertossoberanosar@gmail.com

**Acreditación:**

El presente proyecto es presentado en carácter de autora ciudadana y en cumplimiento de estándares internacionales de Gobierno Abierto, Transparencia Digital y Soberanía de Datos.

# **ANEXO I — SISTEMA DE METRICAS PUBLICAS DE INTEGRIDAD Y ESTABILIDAD ESTRATEGICA (SMPIE)**

## **1. Objeto**

Establecer el conjunto de indicadores agregados, no revelatorios, destinados a brindar a la ciudadanía visibilidad sobre el estado sanitario del patrimonio estratégico de la Nación, sin comprometer información clasificada ni operativa.

## **2. Principios de diseño**

- a) No revelación de volúmenes exactos.
- b) Reflectividad estadística: deben mostrar tendencias sin permitir inferencias sensibles.
- c) Detectabilidad: deben reaccionar ante anomalías abruptas.
- d) Reproducibilidad: los indicadores deben poder recalcularse por terceros autorizados a partir de los tokens de auditoría.
- e) Inalterabilidad: no se admite recálculo manual.

## **3. Conjunto de indicadores**

### **3.1 Índice de Consistencia Patrimonial (ICP)**

- Mide la coherencia entre registros tokenizados, auditorías internas, auditorías externas y curvas históricas.
- Presentación: valor entre 0 y 1.
- Umbráles:
  - 0,95 – 1,00 → “Integridad Óptima”
  - 0,85 – 0,95 → “Integridad Adecuada”
  - < 0,85 → “Alerta de Incoherencia”

### **3.2 Índice de Volatilidad Estratégica (IVE)**

- Mide cambios porcentuales en reservas sin revelar cantidades.
- Usa variaciones normalizadas entre períodos.
- Alerta automática si supera 2 desviaciones estándar respecto a los últimos 12 períodos.

### **3.3 Índice de Riesgo Sistemático (IRS)**

- Evalúa correlación entre reservas estratégicas, deuda pública, tipo de cambio y liquidez fiscal.
- Se publica como escala 0–10.
- Interpretación pública:
  - 0–3 bajo
  - 3–6 moderado
  - 6–10 crítico

### **3.4 Semáforo de Integridad Estratégica (SIE)**

- Representación simplificada del ICP + IVE + IRS.
- Verde: integridad estable.
- Amarillo: anomalías detectadas pero contenidas.
- Rojo: riesgo alto o incoherencia estructural.

### **3.5 Indicador de Anomalía Tokenizada (IAT)**

- Detecta inconsistencias en tokens de auditoría.
- Si  $>0$  indica presencia de eventos no reconciliados (errores, accesos indebidos, alteraciones).

## **4. Frecuencia de publicación**

- Régimen normal: trimestral (90 días).
- Régimen de crisis declarada: mensual (30 días).
- Eventos críticos: publicación inmediata.

## **MATRIZ DE CLASIFICACIÓN DE INFORMACIÓN PARA TOKENIZACIÓN**

Categoría	Descripción	Ejemplos	Nivel de Acceso	Tokenización Permitida
<b>A – Información Pública Abierta</b>	Datos no sensibles, de uso ciudadano presupuestos, estadísticas, catastro		Público total	Total, en cadena pública
<b>B – Información Sensible</b>	Afecta privacidad o identidad	salud, biometría, datos de menores	Acceso restringido	Tokenización en entornos cerrados, sin exportación
<b>C –</b>	Riesgo	inventarios	Acceso técnico	Tokenización con

Categoría	Descripción	Ejemplos	Nivel de Acceso	Tokenización Permitida
<b>Información Reservada</b>	institucional moderado	estatales, contratos energéticos	autorizado	verificación interna
<b>D – Información Clasificada / Secreto de Estado</b>	Riesgo crítico para seguridad nacional	localización reservas de oro, infraestructura crítica	Seguridad/Defensa + auditoría ética ciega	Tokenización por representación sintética, sin exponer detalles

---

## ANEXO II — METODOLOGIA DE TOKENIZACION SOBERANA Y AUDITORIA MULTICAPA

### 1. Objetivo

Definir el estándar técnico mínimo para tokenizar información reservada y generar evidencia verificable sin exponer datos sensibles.

### 2. Características del token soberano

- a) No replicable.
- b) No exportable a infraestructuras extranjeras.
- c) Huella criptográfica verificable por universidades nacionales.
- d) Relación unívoca con un registro interno no publicado.
- e) Resistencia a ataques de correlación o inferencia.

### 3. Capas de auditoría

#### 3.1 Auditoría Interna (Nivel A)

- Validación del Poder Ejecutivo.
- Registro de movimientos, variaciones y accesos.

#### 3.2 Auditoría Externa Institucional (Nivel B)

- Auditoría General de la Nación.
- Cruzamiento con series históricas.

### **3.3 Auditoría Técnica Académica (Nivel C)**

- Universidades nacionales.
- Verificación criptográfica, modelos de riesgo y series temporales.

### **3.4 Auditoría Automatizada (Nivel D)**

- Sistema basado en anomalía tokenizada (IAT).
- Alarmas automáticas ante inconsistencias.

## **4. Condiciones de seguridad**

- Prohibición de despliegue en servicios cloud extranjeros.
- Hardware administrado por el Estado.
- Mecanismos de doble control (two-man rule) para accesos sensibles.

## **INDICADORES PÚBLICOS OBLIGATORIOS SOBRE RESERVAS ESTRATÉGICAS**

### **1. Indicadores Sintéticos Obligatorios (publicación mensual)**

- Índice de Variación Agregada de Reservas Estratégicas (IVARE).
- Índice de Riesgo de Deterioro Estratégico (IRDE).
- Índice de Vulnerabilidad Crítica (IVC).
- Diferencia porcentual entre reservas proyectadas y reservas verificadas criptográficamente.

### **2. Indicadores de Consistencia Operativa (auditados, no públicos)**

- Integridad de almacenamiento seguro.
- Tasa de movimientos operativos autorizados.
- Alertas matemáticas por variación atípica.

### **3. Frecuencia de Publicación**

- Datos públicos: mensual.
  - Datos auditables por Congreso: quincenal.
  - Datos internos críticos: en tiempo real.
-

# **ANEXO III — ESTANDAR DE PUBLICACION CIUDADANA Y TRANSPARENCIA NO REVELATORIA**

## **1. Objetivo**

Garantizar a la ciudadanía información suficiente para evaluar integridad y gobernanza, sin comprometer reservas estratégicas.

## **2. Formato obligatorio de publicación**

La autoridad competente deberá publicar:

- a) Los indicadores del SMPIE (ICP, IVE, IRS, SIE, IAT).
- b) Notas técnicas explicativas.
- c) Gráficos de tendencias (no absolutos).
- d) Informe de auditoría externa e interna (solo conclusiones no clasificadas).
- e) Registro de alarmas emitidas durante el período.

## **3. Datos que no podrán publicarse**

- a) Volúmenes exactos de oro, litio, minerales críticos o combustibles.
- b) Ubicación geográfica exacta de reservas o infraestructura crítica.
- c) Rutas de transporte, seguridad o custodia.
- d) Datos biométricos o identificatorios.

## **4. Derechos de la ciudadanía**

- a) Acceder a métricas verificables.
- b) Presentar solicitudes formales de revisión ante inconsistencias.
- c) Acceder al método de cálculo de los indicadores.
- d) Exigir correcciones si existieran errores detectados por universidades públicas o auditorías independientes nacionales.

## **5. Mecanismo de publicación**

- Portal de Trazabilidad Pública (PTP).
- API pública para consulta de métricas no clasificadas.
- Registro histórico inalterable (5 años mínimo).
- Publicación accesible para personas con discapacidad.

## **TABLEROS DE CONTROL (DASHBOARDS) — MODELOS DE VISUALIZACIÓN**

## **1. Dashboard de Riesgo Soberano**

Componentes:

- Gráfico tipo velocímetro para IRDE.
- Semáforo de riesgo (Verde <5%; Amarillo 5–15%; Naranja 15–30%; Rojo >30%).
- Línea de tendencia histórico-actual-futuro.
- Indicador de correlación entre reservas tokenizadas y patrimonio real.

## **2. Dashboard de Reservas Estratégicas**

Componentes:

- Nube de calor por sector estratégico (oro, litio, agrobiomasa, hidrocarburos).
- Variación porcentual mensual.
- Alerta automática por desvío >2%.

## **3. Dashboard de Trazabilidad Crítica**

Componentes:

- Mapa conceptual sin localización real.
- Flujo de tokens por etapa (extracción → traslado seguro → custodia → auditoría).
- Alertas por operaciones irregulares.

# **ANEXO IV - MÉTRICAS, INDICADORES Y PROTOCOLOS PARA LA TOKENIZACIÓN DE RECURSOS ESTRATÉGICOS Y RESERVAS NACIONALES**

## **1. Finalidad del Anexo**

Este anexo establece las métricas mínimas, indicadores, métodos de publicación y protocolos de auditoría para garantizar transparencia ciudadana sin comprometer la seguridad nacional en la tokenización de recursos estratégicos.

## **2. Principios técnicos aplicados**

- a) Publicación de métricas derivadas sin revelar datos clasificados.
- b) Trazabilidad técnica verificable.
- c) Auditoría ética con doble capa: pública y reservada.
- d) Compatibilidad con estándares de seguridad militar y post-SWIFT.

---

### **3. Categorías de Métricas Obligatorias**

#### **3.1. Métrica de Variación del Stock Estratégico (MVSE)**

Indica la variación porcentual del stock estratégico sin revelar cantidades reales.

Fórmula:

$$\text{MVSE} = ((\text{Token\_Actual} - \text{Token\_Periodo\_Anterior}) / \text{Token\_Periodo\_Anterior}) \times 100$$

Publicación: trimestral.

Permite detectar movimientos irregulares, pérdidas, traspasos no auditados o deterioro.

---

#### **3.2. Índice de Integridad de Reservas Nacionales (IIRN)**

Puntaje de 0 a 1 que indica la integridad técnica y la consistencia del inventario tokenizado.

Componentes internos (no públicos):

- Chequeo de existencia
- Chequeo de pureza / calidad
- Chequeo de ubicación validada
- Trazabilidad de movimientos autorizados
- Registro de accesos clasificados

Publicación: valor agregado trimestral sin detalle interno.

---

#### **3.3. Indicador de Riesgo Geoestratégico (IRG)**

Indicador derivado (no revela volúmenes ni ubicaciones).

Rangos:

0.0–0.3 Riesgo bajo

0.3–0.6 Riesgo medio

0.6–1.0 Riesgo alto

Variables internas consideradas:

- Conflictos geopolíticos en países proveedores
- Movimientos de mercado internacional
- Riesgos de corte de suministro
- Vulnerabilidad de infraestructura crítica
- Presión geoestratégica externa

Publicación: trimestral.

---

### **3.4. Indicador de Anomalías de Trazabilidad (IAT)**

Se publica solo si existe una anomalía.

Tipos:

- a) Anomalía menor
- b) Anomalía moderada
- c) Anomalía crítica

La ciudadanía recibe un aviso del tipo, sin detalles operativos.

---

### **3.5. Health Score Estratégico (HSE)**

Métrica global del estado del sistema de reservas estratégicas tokenizadas.

Incluye:

- Integridad
- Riesgo
- Consistencia
- Alertas activas
- Auditorías aprobadas

Rango: 0–100

Publicación: trimestral.

---

## **4. Protocolo de Publicación Ética y Segura**

### **4.1. Periodicidad:**

- Publicación obligatoria trimestral.
- Informe semestral ampliado.
- Informe anual técnico para Congreso (parte pública y parte reservada).

### **4.2. Formato:**

- Panel público ANDAS
- Dashboard transparente
- Excluye volúmenes, ubicaciones y rutas logísticas
- Incluye: métricas, gráficos derivados, tendencias, alertas

### **4.3. Prohibiciones:**

- No publicar cantidades de oro, litio, energía o minerales.
- No publicar contratos estratégicos específicos.
- No publicar mapas, nodos o rutas críticas.

---

## **5. Auditorías y Supervisión**

- 5.1. Auditoría Técnica Interna:** trimestral.
  - 5.2. Auditoría Universitaria Externa:** anual.
  - 5.3. Auditoría Extraordinaria:** ante alertas críticas del IAT.
  - 5.4. Remisión al Congreso:** versión dividida en pública + reservada.
- 

## **6. Métricas Especiales en Situación Crítica**

Cuando el país se encuentre en:

- riesgo de hiperinflación,
- crisis fiscal severa,
- presión geoestratégica externa,
- estado de emergencia,

se deberán publicar indicadores mensuales derivados para control ciudadano:

- a) MVSE mensual
- b) IRG mensual
- c) HSE mensual
- d) Indicadores de movimientos críticos (sin localización)

Optional: publicación quincenal si el Poder Ejecutivo lo determina.

## **MODELO DE TOKENS SEGÚN TIPO DE ACTIVO**

### **1. Token A – Datos Públicos**

- Abierto, verificable, interoperable.
- Permite auditoría ciudadana directa.

### **2. Token B – Datos Sensibles**

- Encriptación avanzada, acceso por atributos.
- No exportable fuera del territorio nacional.

### **3. Token C – Recursos Estratégicos**

- Incluye metadatos de consistencia, no ubicación.
- Auditoría matemática y ética obligatoria.

### **4. Token D – Reservas Clasificadas**

- Token sintético, no representa cantidad absoluta.
  - Solo representa: variación, riesgo, alertas.
- 

# **ANEXO TÉCNICO V - PROTOCOLOS, INDICADORES Y CAPAS DE SEGURIDAD PARA TOKENIZACIÓN DE DATOS BIOMÉTRICOS Y DATOS SENSIBLES**

## **1. Finalidad del Anexo**

Establecer los estándares mínimos para el manejo, tokenización, protección, anonimización y auditoría de datos biométricos y datos sensibles bajo máxima seguridad nacional.

---

## **2. Capas de Seguridad Obligatorias**

### **2.1. Infraestructura Aislada (Air-Gapped)**

- Servidores sin conexión a internet.
- Aislamiento físico certificado.
- Puentes de transferencia regulados por hardware auditado.

### **2.2. Criptografía de Estado**

- Hashes biométricos irreversibles.
- Salting dinámico.
- Ofuscación múltiple.
- No interoperabilidad con sistemas comerciales.

### **2.3. Registro de Accesos a Nivel Militar**

- Firma digital del operador.
  - Justificación obligatoria por escrito.
  - Validación criptográfica en capas.
- 

## **3. Métricas para Supervisión Ética y Control Estatal**

### **3.1. Índice de Riesgo de Reidentificación (IRR)**

Rango: 0–1

Cálculo interno basado en:

- Robustez del hash
- Posibilidad matemática de reconstrucción
- Exposición accidental
- Integridad del entorno

Publicación: no pública; solo en reporte anual reservado.

---

### **3.2. Indicador de Accesos Sensibles (IAS)**

Métrica pública trimestral:

- Cantidad de accesos autorizados
- Existencia de accesos rechazados
- Existencia de accesos irregulares (sin detalle)

Formatos de reporte:

- a) 0 accesos irregulares
  - b) 1 acceso irregular
  - c) Más de 1 acceso irregular (activar alerta)
- 

### **3.3. Indicador de Consistencia de Anonimización (ICA)**

Controla:

- Aplicación correcta de salting
- Irreversibilidad matemática
- No coincidencia con bases externas
- Estado de los tokens irreversibles

Puntaje interno: 0–100

Publicación: rango general (alto / medio / bajo).

---

## **4. Protocolos Operativos**

### **4.1. Tokenización permitida**

Solo en los casos:

- Identidad digital soberana
- Salud pública
- Seguridad interior
- Investigación judicial
- Emergencias sanitarias y humanitarias

#### **4.2. Tokenización prohibida**

- Empresas extranjeras
  - Nubes externas
  - Plataformas comerciales
  - Tecnologías no auditables
  - Sistemas con IA extranjera entrenada con biometría de terceros
- 

#### **5. Auditoría Externa**

**5.1. Universidades nacionales:** auditoría anual.

**5.2. Organismos independientes:** revisión de protocolo IRR.

**5.3. Inspecciones sorpresa:** habilitadas por la Autoridad de Aplicación.

---

#### **6. Sistema de Alertas Éticas**

Se activa automáticamente cuando:

- a) Hay accesos irregulares.
- b) El IRR supera 0.4.
- c) Fallan los sistemas de aislamiento.
- d) Se detecta intento de exportación o copia no autorizada.

Alertas se clasifican en:

- Verde (normal)
  - Amarillo (riesgo moderado)
  - Rojo (riesgo alto)
  - Negro (incidente crítico)
- 

#### **7. Protección Ciudadana**

Siempre debe estar garantizado:

- Consentimiento informado reforzado.
- Revisión ciudadana de métricas no sensibles.
- Prohibición absoluta de uso comercial o especulativo.
- Derechos de acceso, rectificación y supresión.

### **PROTOCOLO DE AUDITORÍA ÉTICA**

#### **Fases**

1. Recepción de hashes y verificadores matemáticos.

2. Validación cruzada con registros físicos (sin revelar ubicación).
3. Confirmación interinstitucional (Economía, Defensa, Seguridad).
4. Emisión automática de dictamen matemático.
5. Informe narrativo ético para Congreso y sociedad.

### **Tipos de Auditoría**

- Ordinaria: trimestral.
- Extraordinaria: ante riesgo naranja o rojo.
- Forense: ante sospecha de corrupción o manipulación.

# **ANEXO TÉCNICO VI - GOBERNANZA, RESPONSABILIDADES, FLUJOS DE CONTROL Y SUPERVISIÓN DEL ECOSISTEMA NACIONAL DE TOKENIZACIÓN ÉTICA**

## **1. Finalidad del Anexo**

Definir la estructura institucional, los roles, los mandatos, los flujos de supervisión, y los mecanismos de rendición de cuentas para gestionar la tokenización estatal bajo principios de soberanía digital, seguridad nacional, integridad técnica y transparencia ética.

## **2. Arquitectura Institucional Nacional**

### **2.1. Autoridad Nacional de Datos Abiertos y Seguridad (ANDAS)**

(Se podrá designar u otra entidad equivalente si se decide la creación de una Agencia de Tokenización Ética.)

Responsabilidades centrales:

- a) Diseñar estándares, protocolos y lineamientos obligatorios para toda tokenización estatal.
- b) Administrar la infraestructura soberana de datos críticos.
- c) Controlar la trazabilidad ética de todos los procesos descritos en la ley.
- d) Autorizar, supervisar y auditar las tokenizaciones de:
  - Datos públicos
  - Datos sensibles

- Reservas estratégicas
- Infraestructura crítica
- e) Emitir los informes trimestrales, semestrales y anuales (públicos y reservados).
- f) Mantener un registro nacional de proyectos y sistemas basados en tokenización estatal.
- g) Activar protocolos de alerta temprana ante anomalías o incidentes críticos.

## **2.2. Consejo Federal de Tokenización Ética (CFTE)**

Órgano consultivo y federal integrado por:

- Representantes designados por las provincias
- Universidades nacionales
- Organismos científicos
- Equipos técnicos especializados

Funciones:

- a) Revisión técnica anual de estándares de seguridad.
- b) Evaluación del impacto federal de la tokenización.
- c) Recomendaciones públicas no vinculantes.
- d) Coordinación de interoperabilidad soberana entre jurisdicciones.

## **2.3. Auditoría Externa Universitaria Nacional**

Las universidades nacionales designadas actuarán como tercera línea independiente, con funciones de:

- a) Auditoría anual obligatoria.
- b) Revisión de métricas y algoritmos utilizados en tokens derivados.
- c) Evaluación de riesgos de reidentificación y consistencia.
- d) Control criptográfico externo.
- e) Participación en informes al Congreso.

## **2.4. Órgano de Supervisión Parlamentaria de la Tokenización Ética (OSPT)**

Cámara de Diputados + Senado — Comisión Bicameral.

Atribuciones:

- a) Recibir informes anuales (públicos y reservados).
- b) Convocar a ANDAS a comparecer por anomalías o incidentes críticos.
- c) Requerir auditorías extraordinarias.
- d) Emitir recomendaciones vinculantes en caso de vulneración de seguridad nacional.

## **3. Líneas de Responsabilidad y Control**

### **3.1. Primera Línea (Operativa):**

Equipos técnicos estatales que ejecutan:

- Tokenización
- Anonimización
- Validación
- Publicación de métricas
- Generación de tokens de auditoría

### **3.2. Segunda Línea (Supervisión):**

ANDAS / Agencia especializada

- Control técnico
- Alertas
- Revisión de accesos
- Validación de la infraestructura
- Coordinación federal

### **3.3. Tercera Línea (Auditoría Independiente):**

- Universidades
- Expertos científicos
- Institutos tecnológicos nacionales

### **3.4. Cuarta Línea (Control Democrático):**

- Ciudadanía (informes públicos)
  - Parlamento (informes reservados y citaciones)
- 

## **4. Protocolos de Actuación ante Incidentes**

Clasificaciones:

- Nivel Verde: funcionamiento normal
- Nivel Amarillo: riesgo moderado
- Nivel Rojo: riesgo alto
- Nivel Negro: incidente crítico con afectación potencial de soberanía

Acciones:

- a) ANDAS activa auditoría interna urgente.
  - b) Se convoca auditoría universitaria extraordinaria.
  - c) Se notifica a la Comisión Bicameral del Congreso.
  - d) Se suspende o congela el módulo comprometido.
  - e) Si hay fuga o intento de exportación: intervención inmediata + denuncia penal.
-

## **5. Informes y Rendición de Cuentas**

Periodicidades:

- Trimestral público para ciudadanía
  - Semestral técnico intermedio
  - Anual integral con doble cuerpo: público + reservado para Congreso
  - Informe extraordinario ante incidentes críticos
- 

## **6. Mapa Federal de Interoperabilidad**

Incluye:

- Provincias
- Municipios críticos
- Regiones con reservas estratégicas
- Instituciones educativas vinculadas
- Nodos de infraestructura nacional

Se prohíbe cualquier vínculo con infraestructuras tecnológicas extranjeras.

## **ALGORITMO DE DETECCIÓN TEMPRANA DE RIESGO SISTÉMICO**

### **Variables Consideradas**

- Variación anómala de reservas (percentil 95).
- Señales macroeconómicas de estrés (inflación esperada >8% mensual).
- Distorsiones en trazabilidad.
- Alertas de ciberseguridad de infraestructura crítica.
- Indicadores de desabastecimiento esencial.

### **Salida del algoritmo**

- Nivel de riesgo (verde/amarillo/naranja/rojo).
  - Lista de activos en alerta.
  - Recomendaciones automáticas.
- 

## **ANEXO VII - LICENCIAMIENTO SOBERANO, ESTÁNDARES**

# **ABIERTOS, PROTOCOLOS DE NO EXPORTACIÓN Y PROHIBICIÓN DE DEPENDENCIA TECNOLÓGICA**

## **1. Finalidad del Anexo**

Definir el modelo de licenciamiento, protección del software, infraestructura, algoritmos, tokens, paneles, dashboards y herramientas derivadas del presente régimen legal, garantizando independencia técnica, soberanía criptográfica y no dependencia de terceros.

## **2. Principios Fundamentales del Licenciamiento Soberano**

### **2.1. No exportación de infraestructura estratégica**

Queda prohibido que cualquier componente de:

- Tokenización
- Infraestructura
- Algoritmos críticos
- Bases de datos
- Identidad digital
- Sistemas biométricos

sea alojado, gestionado, auditado o controlado fuera del territorio argentino.

### **2.2. Licencias estatales libres compatibles**

El Estado deberá utilizar licencias que permitan:

- a) Revisión pública del código correspondiente a las partes no sensibles.
- b) Auditoría técnica por universidades y organismos científicos.
- c) Protección contra uso comercial indebido.
- d) Protección contra cierre tecnológico.

Ejemplo de esquemas posibles:

- Licencia Pública Nacional Argentina (LPNA)
- Variantes adaptadas de GPL, AGPL o EUPL con cláusulas de seguridad nacional
- Esquemas híbridos con módulos reservados (criptografía, infraestructura crítica)

### **2.3. No dependencia y no lock-in tecnológico**

Los sistemas no podrán utilizar:

- Infraestructura provista por Big Tech
- Nubes extranjeras
- APIs cerradas bajo jurisdicción extranjera

- Sistemas propietarios inauditables
- Dependencias técnicas no documentadas

El software deberá ser migrable, auditible y replicable en infraestructura estatal.

---

### **3. Licenciamiento del Código Crítico**

El código crítico comprende:

- Criptografía
- Módulos de anonimización
- Protocolos de trazabilidad
- Software de seguridad nacional
- Algoritmos de tokenización

Normativa:

- a) Solo podrá ser auditado por universidades nacionales designadas.
  - b) No podrá publicarse ni divulgarse.
  - c) Se mantendrá bajo licencia soberana restringida.
  - d) Su exportación constituye delito federal agravado.
- 

### **4. Licencias para Software No Crítico**

Este incluye:

- Dashboards públicos
- Parámetros visuales
- Métricas derivadas
- Paneles ciudadanos
- Documentación
- Metodologías públicas

Debe utilizar licencias abiertas que permitan:

- Reutilización
- Auditoría
- Reimplementación
- Adaptación regional

Sin permitir:

- Uso comercial especulativo
  - Reventa
  - Tokenización financiera privada
-

## **5. Licenciamiento de Tokens**

Los tokens emitidos bajo este régimen se clasifican:

### **5.1. Tokens Públicos Derivados**

- No son financieros
- No son comerciables
- No generan valor especulativo
- Solo representan métricas, integridad y estado del sistema
- Su licencia prohíbe explícitamente:
  - a) compra
  - b) venta
  - c) mercado secundario
  - d) exchanges
  - e) staking
  - f) financiamiento colateral

### **5.2. Tokens de Auditoría Soberana**

- Acceso reservado
  - Licencia de uso interno
  - Intransferibles
  - No interoperables
  - Prohibición absoluta de exportación
  - Protección penal agravada
- 

## **6. Documentación Técnica Obligatoria**

Todo sistema basado en esta ley debe contar con:

- a) Manual técnico
  - b) Manual de operaciones
  - c) Registro de dependencias
  - d) Auditorías criptográficas
  - e) Plan de migración
  - f) Plan de contingencia
  - g) Especificación de licencias aplicadas
  - h) Registro de terceros autorizados
- 

## **7. Incompatibilidades**

No podrá utilizarse nada que involucre:

- Amazon AWS
  - Google Cloud
  - Azure
  - Oracle Cloud
  - IBM Cloud
  - Infraestructuras chinas o estadounidenses no auditables
  - SAAS foreign-hosted
  - Frameworks cerrados con telemetría oculta
- 

## **8. Esquema de Cumplimiento**

Todo organismo público deberá presentar:

- Informe anual de licencias
- Verificación de independencia tecnológica
- Matriz de riesgos de dependencia
- Certificado de interoperabilidad soberana

ANDAS certificará su cumplimiento.

## **PROCEDIMIENTO TÉCNICO PARA ACTIVAR EL PNET (PROTOCOLO DE EMERGENCIA)**

### **Etapa 1 – Verificación**

- Doble comprobación matemática.
- Confirmación humana de un organismo independiente.

### **Etapa 2 – Notificación**

- Al Poder Ejecutivo.
- Al Congreso.
- A Seguridad y Defensa.
- A organismos multilaterales si corresponde.

### **Etapa 3 – Escalonamiento**

- Nivel amarillo: refuerzo de auditoría.
- Nivel naranja: control conjunto.
- Nivel rojo: Comando Unificado.

### **Etapa 4 – Ejecución**

- Activación de modo de infraestructura degradada (si aplica).
- Asignación segura de recursos humanitarios.
- Protección física de reservas sensibles.

#### **Etapa 5 – Cierre y Normalización**

- Auditoría final.
- Publicación de informe síntesis.
- Restablecimiento del régimen ordinario.

## **ANEXO VIII. PROTOCOLOS DE PUBLICACIÓN DE SERIES CRÍTICAS DE DATOS EN CONTEXTOS DE EMERGENCIA**

### **1. Objetivo**

Establecer los mecanismos, plazos y formatos para la publicación de información crítica en situaciones de riesgo extremo: hiperinflación, corrida cambiaria, fuga de capitales, desabastecimiento, caída de reservas estratégicas o riesgos de impacto humanitario.

### **2. Series críticas obligatorias**

Las siguientes métricas deberán publicarse en **plazos acelerados**, aun cuando parte de la información sea clasificada.

En dichos casos, se garantiza publicación de **agregados y variaciones**, nunca el volumen absoluto.

#### **2.1. Monetarias y macrofinancieras**

- Índice de Precios al Consumidor (variación semanal durante crisis).
- Base Monetaria (variación semanal).
- Agregados Monetarios M1 y M2 (variación semanal).
- Riesgo país.
- Tipo de cambio oficial, financiero y paralelo (brechas).
- Flow de capitales y presión sobre reservas (indicadores sintéticos, no montos).

#### **2.2. Reservas estratégicas**

- Oro físico: variación porcentual quincenal.

- Minerales críticos (litio, cobre, gas, petróleo): tasa de extracción, exportación y existencias relativas.
- Reservas de combustibles: variación porcentual semanal.

### 2.3. Indicadores sociales

- Línea de pobreza y canasta básica (actualización quincenal).
- Acceso a alimentos esenciales y medicamentos (índice de abastecimiento semanal).
- Riesgo de emergencia humanitaria: modelo sintético (baseline vs. estrés).

### 2.4. Operaciones del Estado tokenizadas

- Emisiones nuevas, cancelaciones, retiros y auditorías (publicación automática diaria).
  - Movimientos de contratos tokenizados: indicadores de integridad.
- 

## 3. Plazos de publicación en situación crítica

- **Diario:** tipo de cambio, brechas, presión cambiaria, actividad del sistema tokenizado.
  - **Semanal:** IPC adelantado, M2, abastecimiento, reservas sintéticas.
  - **Quincenal:** pobreza, variación de reservas estratégicas agregadas.
  - **Mensual:** auditoría integral del sistema y verificadores criptográficos.
- 

## 4. Formatos

- **Machine-readable:** CSV + JSON-LD + API REST gubernamental.
  - **Tableros abiertos:** panel con indicadores, alertas automáticas y gráfico de riesgo.
  - **Históricos descargables:** series completas desde el inicio de la implementación.
- 

## MATRIZ DE DECISIÓN PARA REDISTRIBUCIÓN HUMANITARIA DE ACTIVOS

Escenario	Condición	Acción sobre Activos	Auditoría	Comunicación
Crisis alimentaria	desabastecimiento $\geq 10\%$	Redistribución tokenizada inmediata	Ética extraordinaria	Informe diario
Crisis energética	fallas $\geq 20\%$ en red	Movilización	Conjunta con	Alerta nacional

<b>Escenario</b>	<b>Condición</b>	<b>Acción sobre Activos</b>	<b>Auditoría</b>	<b>Comunicación</b>
		prioritaria de combustible	Defensa	
Hiperinflación crítica	inflación mensual >30%	Activación reservas estabilizadoras	Económica + Ética	Boletín técnico
Evento bélico/ciberataque	infraestructura degradada	Reforzamiento de custodia	Defensa + Ciberseguridad	Comunicación controlada

## **ANEXO IX - MODELO DE AUDITORÍA ÉTICA Y TRAZABILIDAD MULTINIVEL (MET)**

### **1. Objetivo**

Garantizar que ningún dato crítico, aunque sea clasificado, quede sin supervisión independiente y trazabilidad criptográfica.

### **2. Capas de auditoría**

#### **2.1. Auditoría Ciega Criptográfica ( nivel interno )**

- El Estado registra los valores reales en un **contenedor cifrado de alta seguridad**.
- Los auditores acceden solo a verificadores matemáticos (hashes, ZK-proofs).
- Ninguna persona ve los datos sensibles en forma explícita.

#### **2.2. Auditoría Ética Multilateral ( nivel externo )**

Integrada por:

- Universidades públicas.
- Organismos multilaterales.
- Expertos independientes del Registro Ético Nacional.

Todos verifican consistencia de:

- Flujos reales vs. publicados.
- Ausencia de manipulación.
- Cumplimiento de plazos y calidad de las series.

### **2.3. Auditoría Ciudadana ( nivel público )**

- Herramientas de verificación para que cualquier ciudadano compruebe que la **serie oficial coincide con el hash publicado** en la cadena estatal.
- 

### **3. Mecanismo de trazabilidad**

- Todas las operaciones del ecosistema tokenizado generan un hash público.
  - Se incluyen metadatos mínimos necesarios para control sin exponer datos sensibles.
  - Los quiebres de trazabilidad generan “alertas rojas” obligatorias con:
    - Notificación al Congreso.
    - Notificación a organismos multilaterales.
    - Notificación al Registro Ético Nacional.
- 

### **4. Sanciones por manipulación**

- Suspensión automática del funcionario responsable.
  - Auditoría extraordinaria obligatoria.
  - Derivación judicial con agravante por “afectación a la integridad del Sistema Ético de Datos Críticos”.
- 

## **ANEXO X - MARCO TECNOLÓGICO PARA TOKENIZACIÓN ÉTICA**

### **1. Componentes del ecosistema**

#### **1.1. Cadena estatal de confianza**

- Blockchain pública-permissionada
- Gobernanza institucional
- Hashes visibles para ciudadanía
- ZK-proofs para datos clasificados

#### **1.2. Monitoreo automático**

- Módulo de alertas tempranas ante:
  - inflación acelerada

- deterioro de reservas
- fuga de capitales
- manipulación de series
- cambios abruptos en operaciones tokenizadas

### **1.3. Registro Ético Nacional**

- Administra identidades verificadas
  - Licencias de operadores
  - Listado de expertos habilitados para auditorías externas
- 

### **2. Estándares técnicos requeridos**

- ISO/IEC 27001 (seguridad).
  - ISO 37120 (indicadores urbanos y sociales).
  - Open Contracting Data Standard (OCDS) para contrataciones tokenizadas.
  - Estándar global para datos de reservas (GRG-RDS) en versión pública y sintética.
- 

### **3. Requerimientos de interoperabilidad**

- Integración con:
    - API monetaria del BCRA (modo sintético).
    - API de energía y minería.
    - API de desarrollo social.
    - Plataforma de compras públicas tokenizadas.
  - Todos los sistemas deberán exponer:
    - endpoints públicos
    - endpoints internos con trazabilidad completa
    - endpoints de auditoría ciega criptográfica
- 

### **4. Minimización de riesgos tecnológicos**

- Redundancia nacional + espejo internacional en organismo neutral.
- Pruebas de estrés trimestrales.
- Pruebas de integridad criptográfica continuas.
- Mecanismo de desconexión segura ante ataques sin pérdida de trazabilidad.

## **Trazabilidad y tokenización ética de la sostenibilidad digital y ciudadana.**

La **Agencia Nacional de Datos Abiertos y Soberanos (ANDAS)** podrá desarrollar e implementar mecanismos de **tokenización ética y soberana** de los indicadores ambientales, energéticos y de sostenibilidad derivados de la **Certificación de Entidad Digital Verde (EDV)** y de las acciones sostenibles de los ciudadanos, con el objeto de promover conductas responsables, eficiencia energética y participación ecológica en el ámbito digital.

- a) Los **tokens verdes soberanos** representarán valores verificables de **cumplimiento ambiental y conducta sostenible**, sin carácter financiero ni especulativo, emitidos exclusivamente sobre bases de datos auditadas y certificadas por la **ANDAS** y el **Ministerio de Ambiente y Desarrollo Sostenible**.
- b) Los organismos públicos, instituciones educativas y proveedores de bienes o servicios podrán integrarse al sistema de tokenización ética para **reconocer, recompensar o incentivar acciones de sostenibilidad** (reciclaje, ahorro energético, consumo responsable, participación digital verde, uso de servicios certificados).
- c) Los ciudadanos que participen en programas, plataformas o servicios certificados como sostenibles podrán **recibir beneficios tangibles**, tales como:
  1. **Bonificaciones o créditos verdes** aplicables a tarifas de transporte, energía o servicios públicos;
  2. **Descuentos en bienes y servicios** producidos o distribuidos por entidades con Certificación EDV;
  3. **Acceso prioritario a programas de educación ambiental, innovación digital o becas verdes**;
  4. **Reconocimiento fiscal o compensación parcial de tasas locales o provinciales** cuando se acredite reducción de huella ecológica o participación en reciclaje tecnológico.
- d) La tokenización se basará en **principios de transparencia, soberanía tecnológica y protección de datos personales**, utilizando infraestructura estatal o software libre auditado, alojado en la **Nube Pública Nacional (NPN)**.
- e) Los tokens verdes soberanos serán **de libre acceso y consulta pública**, interoperables con el **Sistema de Trazabilidad Ambiental Digital (STAD)**, y servirán para **medir y visibilizar el impacto ambiental positivo de las acciones ciudadanas y estatales**, sin crear perfiles personales ni mecanismos de vigilancia.
- f) La **ANDAS**, en coordinación con el **Ministerio de Economía**, la **AAIP** y el **Ministerio de Ambiente y Desarrollo Sostenible**, reglamentará el sistema de incentivos y beneficios asociados, garantizando **equidad territorial, respeto a la privacidad y control público** sobre los datos de tokenización.

g) Los beneficios obtenidos por participación ciudadana en programas verdes se financiarán mediante el **Fondo Nacional de Innovación y Sostenibilidad Digital**, creado en el marco de esta ley, integrado por reasignaciones presupuestarias TIC, cooperación internacional y aportes voluntarios de entidades certificadas EDV.

**h) Remediación y Reutilización Ética de Datos Colectados Sin Consentimiento.**

Dispónese la **suspensión inmediata** de cualquier funcionalidad de compartición automática de red, rastreo por firmware, escucha o telemetría domiciliaria activada sin consentimiento.

Créase, con carácter urgente, el **Registro Nacional de Datos Invasivos (RNDI)** bajo la ANDAS, para inventariar y clasificar todo dato recolectado por proveedores de conectividad y operadores móviles que pueda afectar la privacidad domiciliaria o la localización de personas.

La ANDAS, en colaboración con la DNDD y universidades públicas, publicará un informe público en 90 días que describa alcance, responsables y volumen de los datos.

**Prohibición de reutilización y remediaciόn obligatoria**

Queda **prohibida** la reutilización para fines de tokenización, comercialización, publicidad, subsidio o reconocimiento público de **datos personales recolectados sin consentimiento** o sin base legal expresamente prevista.

Los titulares afectados tendrán derecho a que esos datos sean **eliminados** o, en su defecto, **aislados** en custodia restringida si existiera obligación legal de conservación.

Se crea un **Fondo de Reparación y Compensación (FRC)** alimentado por sanciones impuestas a los proveedores infractores y por el FONDAS, para financiar medidas de reparación colectiva (créditos, tarifas o programas) cuando proceda y según opt-in del titular.

**Opt-in retroactivo para reutilización ética y tokenización ciudadana**

Solamente tras la auditoría pública y la notificación expresa, los titulares podrán **optar** (opt-in) por autorizar que **versiones agregadas y probadamente anonimizadas** de sus datos formen parte de programas de tokenización ética o de beneficios verdes.

El consentimiento será **específico, informado y revocable**, con interfaz digital accesible, registro de la aceptación y prueba de autenticidad (firma electrónica o equivalente).

La ANDAS dictará estándares mínimos de anonimización (incluyendo privacidad diferencial cuando proceda) y dejará constancia pública de los parámetros usados.

## **Prohibición de uso de datos sensibles para tokenización**

Se prohíbe terminantemente el uso, incluso con consentimiento, de **datos biométricos, audio de interiores, geolocalización a nivel residencial** o cualquier información que pueda identificar de forma directa la vivienda del titular, para programas de tokenización o recompensas.

Cualquier excepción deberá contar con **autorización judicial previa** y justificación estricta.

## **Mecanismos de beneficio y financiación**

Los beneficios materiales derivados de programas voluntarios de tokenización verde (bonificaciones, créditos, descuentos) deberán financiarse desde el **Fondo Nacional de Innovación y Sostenibilidad Digital** o por recursos sancionatorios a proveedores que hayan vulnerado la normativa.

No se permitirá que las empresas privadas financien beneficios con la condición de recibir datos personales sin pasar por el proceso de opt-in y anonimización.

## **Supervisión, sanciones y medidas compensatorias**

La ANDAS y la DNDD, con apoyo de la AAIP, serán responsables de verificar el cumplimiento.

El uso ilícito o la reutilización no autorizada dará lugar a sanciones administrativas, multas y obligación de reparación individual y colectiva.

Los titulares tendrán acción de amparo preferente ante violaciones graves.

## **Medidas técnicas imprescindibles**

- **Validador de anonimización** (herramienta pública que testea riesgo de reidentificación).
- **Privacidad diferencial** para estadísticas y modelos.
- **Hashing/salting y agregación** antes de cualquier token.
- **Logs públicos** de quién solicitó qué, cuándo, con qué consentimiento.
- **Interfaz ciudadana** para dar, revocar o auditar consentimientos (DNDD/ANDAS).

## **Ejemplo de flujo práctico — cómo sería para un ciudadano**

1. Se detectó que tu ISP activó hotspot sin permiso → ENACOM/ANDAS obliga desactivación.

2. Auditoría identifica que existieron logs de localización → ISP debe borrar o aislar.
3. Se te notifica: “si aceptás, podemos usar una versión agregada ANÓNIMA de tus datos para el programa X; beneficios: descuento en tarifa eléctrica del 5% por 6 meses”.
4. Si aceptás (opt-in), se firma digitalmente; tus datos pasan por privacidad diferencial; recibís token / crédito verificable.
5. En cualquier momento podés revocar; si revocas, se suspende la próxima emisión y se detiene uso futuro.

### **Conclusión — postura recomendada para la ley**

- **Sí a la reparación y a que la ciudadanía reciba beneficios reales** si así lo decide;
- **No a la reutilización automática** de datos colectados sin consentimiento;
- **Sí a un proceso público, auditible y opt-in** con anonimización robusta y estándares técnicos;
- **Sí a un Fondo y a sanciones** que financien la reparación cuando la violación ya ocurrió.

## **PROYECTO DE LEY**

### **Ley de Transparencia y Beneficiarios Reales de Argentina – 2025**

#### **Autora:**

Natividad Vidal

Capilla del Monte, Córdoba, Argentina

**Correo Institucional:** [datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

#### **Presentado ante:**

Honorable Cámara de Diputados de la Nación

Honorable Cámara de Senadores de la Nación

**Fecha:** \_\_\_\_\_ (colocar al momento de presentación)



Natividad Vidal

DNI 27.716.481

Proyecto presentado para su tratamiento en el marco del Programa de Soberanía Digital Argentina, alineado con estándares ONU – CEPAL – OGP.

## **PARTE I**

- **ÍNDICE GENERAL**
- **TÍTULO I – DISPOSICIONES GENERALES**
- **TÍTULO II – SUJETOS OBLIGADOS**
- **TÍTULO III – REGISTRO Y DATOS ABIERTOS**
- **TÍTULO IV – ACTUALIZACIÓN, VERIFICACIÓN Y AUDITORÍA**
- **TÍTULO V – RÉGIMEN SANCIONATORIO**
- **TÍTULO VI – ARTICULACIÓN ESTRATÉGICA**
- **TÍTULO VII – DISPOSICIONES FINALES**
- **FUNDAMENTOS**

## **PARTE II**

- **FIRMADOS**

## **PARTE III**

- **ANEXO I - UMBRALES, CRITERIOS DE CONTROL Y DETERMINACIÓN DEL BENEFICIARIO REAL**
- **ANEXO II - ESTRUCTURAS COMPLEJAS, OFFSHORE Y VEHÍCULOS ESPECIALES**
- **ANEXO III - INTEROPERABILIDAD, DATOS ABIERTOS Y ESTÁNDAR TÉCNICO**
- **ANEXO IV - PROTECCIÓN DE DATOS, SEGURIDAD Y USO LEGÍTIMO**
- **ANEXO V - RÉGIMEN DE REGULARIZACIÓN VOLUNTARIA Y TRANSICIÓN**

# **PROYECTO DE LEY DE TRANSPARENCIA Y BENEFICIARIOS REALES**

## **TÍTULO I – DISPOSICIONES GENERALES**

### **Artículo 1º – Objeto**

La presente ley tiene por objeto establecer el **régimen nacional obligatorio de identificación, registro, publicación y verificación de los beneficiarios reales** de personas jurídicas, estructuras legales y entidades que operen en la República Argentina o mantengan vínculos económicos relevantes con el Estado nacional.

---

### **Artículo 2º – Definición de Beneficiario Real**

Se considera beneficiario real a toda persona humana que, directa o indirectamente:

- a) Posea, controle o sea titular de al menos el **10% del capital, derechos de voto o beneficios económicos**, o
- b) Ejercite **control efectivo**, influencia dominante o poder de decisión, aun sin participación formal, o
- c) Sea beneficiaria final de fideicomisos, trusts, fundaciones privadas u otras estructuras jurídicas.

En ningún caso se admitirá como beneficiario real a otra persona jurídica.

---

## TÍTULO II – SUJETOS OBLIGADOS

### Artículo 3° – Alcance subjetivo

Quedan obligados al cumplimiento de la presente ley:

- a) Personas jurídicas constituidas en el país.
  - b) Sucursales de entidades extranjeras.
  - c) Fideicomisos, trusts, fondos de inversión y estructuras análogas.
  - d) Entidades que accedan a subsidios, beneficios fiscales, contratos públicos o regímenes promocionales (incluido el RIGI).
  - e) Entidades que participen en operaciones con activos estratégicos externos.
- 

### Artículo 4° – Condición habilitante

La identificación y publicación de beneficiarios reales será **condición previa y obligatoria** para:

- contratar con el Estado,
  - acceder a beneficios fiscales o financieros,
  - participar en regímenes especiales de inversión,
  - recibir fondos públicos o internacionales.
- 

## TÍTULO III – REGISTRO Y DATOS ABIERTOS

### Artículo 5° – Registro Nacional de Beneficiarios Reales

Créase el **Registro Nacional de Beneficiarios Reales (RNBR)**, integrado al Sistema Nacional de Datos Soberanos Abiertos.

---

### Artículo 6° – Estándar técnico

El registro adoptará el **Beneficial Ownership Data Standard (BODS)**, garantizando:

- interoperabilidad,
  - trazabilidad histórica,
  - identificadores únicos,
  - publicación en formatos abiertos.
- 

### **Artículo 7° – Publicidad y protección**

Los datos serán públicos, con resguardo de información sensible, sin afectar:

- la identificación del beneficiario real,
  - el porcentaje de control,
  - la estructura de propiedad.
- 

## **TÍTULO IV – ACTUALIZACIÓN, VERIFICACIÓN Y AUDITORÍA**

### **Artículo 8° – Actualización obligatoria**

La información deberá actualizarse:

- a) Anualmente, y
  - b) Dentro de los 30 días ante cualquier cambio relevante.
- 

### **Artículo 9° – Verificación interinstitucional**

La AFIP, UIF, IGJ, Banco Central y autoridad de datos abiertos deberán:

- cruzar información automáticamente,
  - detectar inconsistencias,
  - emitir alertas tempranas.
-

# **TÍTULO V – RÉGIMEN SANCIONATORIO**

## **Artículo 10° – Incumplimientos**

Constituyen infracciones:

- a) Omisión de declaración,
  - b) Falsedad u ocultamiento,
  - c) Uso de estructuras para encubrimiento.
- 

## **Artículo 11° – Sanciones**

Las sanciones podrán incluir:

- multas proporcionales,
- suspensión de beneficios,
- inhabilitación para contratar con el Estado,
- exclusión de regímenes promocionales.

Cuando corresponda, se dará intervención penal.

---

# **TÍTULO VI – ARTICULACIÓN ESTRATÉGICA**

## **Artículo 12° – Integración normativa**

La presente ley se articula con:

- Ley de Activos Estratégicos Externos,
  - Ley de Datos Abiertos Soberanos,
  - Ley de Acceso a la Información Pública,
  - Ley de Prevención de Lavado de Activos,
  - RIGI y sus ampliaciones.
-

### **Artículo 13° – Cooperación internacional**

La autoridad de aplicación promoverá acuerdos de intercambio automático de información conforme estándares OCDE y GAFI.

---

## **TÍTULO VII – DISPOSICIONES FINALES**

### **Artículo 14° – Gradualidad**

La reglamentación establecerá cronogramas progresivos según tamaño y sector.

---

### **Artículo 15° – Entrada en vigencia**

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

## **Fundamentos**

La presente iniciativa busca consolidar una arquitectura de transparencia estructural para el Estado argentino, alineando las prácticas nacionales con los estándares internacionales de gobernanza abierta. El Beneficial Ownership Data Standard (BODS) constituye una herramienta clave para garantizar que los recursos públicos, incluidos los préstamos internacionales y subsidios, se asignen y utilicen de manera trazable y verificable.

Asimismo, la adopción de BODS permitirá a la ciudadanía ejercer control efectivo sobre las estructuras empresariales que concentran beneficios fiscales, contribuyendo a la soberanía digital, la equidad económica y la integridad institucional.

**Firmado:**

**Natividad Vidal**

Autora del Proyecto

Capilla del Monte, Córdoba, Argentina

**Firma manuscrita digital:**



Natividad Vidal

DNI 27.716.481

**Correo institucional:**

[datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

**Acreditación:**

El presente proyecto es presentado en carácter de autora ciudadana y en cumplimiento de estándares internacionales de Gobierno Abierto, Transparencia Digital y Soberanía de Datos.

# **ANEXO I - UMBRALES, CRITERIOS DE CONTROL Y DETERMINACIÓN DEL BENEFICIARIO REAL**

## **Umbral de participación relevante**

Se considerará beneficiario real a toda persona humana que posea directa o indirectamente:

- a) **10 % o más** del capital social,
- b) **10 % o más** de los derechos de voto, o
- c) **10 % o más** de los beneficios económicos.

El umbral se aplicará **de forma acumulativa**, incluyendo participaciones indirectas y encadenadas.

---

## **Control efectivo sin participación formal**

Será considerado beneficiario real quien, aun sin alcanzar el umbral porcentual:

- a) ejerza control mediante pactos privados,
  - b) tenga poder de designación de autoridades,
  - c) influya decisivamente en decisiones estratégicas,
  - d) controle flujos financieros relevantes.
- 

## **Beneficiario residual**

Cuando no pueda identificarse un beneficiario real bajo los criterios anteriores, se deberá declarar como tal a la **máxima autoridad administrativa**, sin perjuicio de continuar la investigación de control efectivo.

---

# **ANEXO II - ESTRUCTURAS COMPLEJAS, OFFSHORE Y VEHÍCULOS ESPECIALES**

## **Trusts, fideicomisos y figuras análogas**

En estructuras fiduciarias deberán declararse:

- a) fideicomitente,
- b) fiduciario,
- c) beneficiario/s,
- d) protector o figuras equivalentes.

Se identificará como beneficiario real a quien tenga **derecho económico final o poder de control**.

---

## **Sociedades offshore y holdings**

Cuando existan sociedades radicadas en el exterior:

- a) se deberá reconstruir la **cadena completa de propiedad**,
- b) identificar jurisdicción, finalidad y sustancia económica,
- c) declarar beneficiario real final persona humana.

No se admitirá la opacidad por secreto societario extranjero.

---

## **Fondos de inversión y vehículos colectivos**

En fondos de inversión se declararán beneficiarios reales cuando:

- a) un inversor supere el umbral legal, o
  - b) ejerza control decisorio, o
  - c) reciba beneficios económicos predominantes.
-

# **ANEXO III - INTEROPERABILIDAD, DATOS ABIERTOS Y ESTÁNDAR TÉCNICO**

## **Estándar de datos**

El Registro adoptará el **Beneficial Ownership Data Standard (BODS)** y formatos abiertos, garantizando:

- identificadores únicos,
  - trazabilidad histórica,
  - control de versiones,
  - interoperabilidad internacional.
- 

## **Integración sistémica**

El Registro se integrará con:

- AFIP,
  - UIF,
  - IGJ / registros provinciales,
  - Banco Central,
  - SINDASA (Datos Abiertos Soberanos).
- 

## **Publicación diferenciada**

Se publicará:

- a) información estructural y agregada para control ciudadano,
  - b) información individual completa para organismos de control.
-

# **ANEXO IV - PROTECCIÓN DE DATOS, SEGURIDAD Y USO LEGÍTIMO**

## **Principio de proporcionalidad**

La publicidad de datos deberá:

- a) garantizar la identificación del beneficiario real,
  - b) evitar exposición innecesaria,
  - c) respetar derechos personales sin afectar el interés público.
- 

## **Información sensible**

Podrá restringirse exclusivamente:

- domicilio exacto,
- datos biométricos,
- información no relevante para control económico.

Nunca podrá ocultarse la identidad del beneficiario real.

---

## **Uso legítimo**

Los datos no podrán utilizarse para:

- a) persecución política,
  - b) discriminación,
  - c) fines ajenos al control público y económico.
-

# **ANEXO V - RÉGIMEN DE REGULARIZACIÓN VOLUNTARIA Y TRANSICIÓN**

## **Regularización inicial**

Durante los primeros **12 meses**, los sujetos obligados podrán:

- a) declarar beneficiarios reales omitidos,
  - b) corregir información incompleta,
  - c) transparentar estructuras complejas.
- 

## **Beneficios por adhesión**

La adhesión voluntaria podrá implicar:

- reducción de sanciones administrativas,
- mantenimiento de beneficios vigentes,
- prioridad en regímenes promocionales.

No aplica a delitos graves.

---

## **Fin del régimen transitorio**

Vencido el plazo, el régimen sancionatorio se aplicará plenamente.

# **PROYECTO DE LEY**

## **Ley de Declaracion Obligatoria de Activos Estrategicos Externos de Argentina – 2025**

### **Autora:**

Natividad Vidal

Capilla del Monte, Córdoba, Argentina

**Correo Institucional:** [datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

### **Presentado ante:**

Honorable Cámara de Diputados de la Nación

Honorable Cámara de Senadores de la Nación

**Fecha:** \_\_\_\_\_

Proyecto presentado para su tratamiento en el marco del Programa de Soberanía Digital Argentina, alineado con estándares ONU – CEPAL – OGP.

## **INDICE GENERAL**

### **PARTE I — TEXTO DEL PROYECTO DE LEY**

- **TÍTULO I – DEFINICIONES Y SUJETOS OBLIGADOS**
- **TÍTULO II – ALCANCE DE LA DECLARACIÓN OBLIGATORIA**
- **TÍTULO III – INFORMACIÓN ABIERTA Y AUDITABLE**
- **TÍTULO IV – BANCA PÚBLICA Y PRIVADA COMO INFRAESTRUCTURA ESTRATÉGICA**
- **TÍTULO V – RÉGIMEN DE REINVERSIÓN Y LIQUIDACIÓN MÍNIMA**
- **TÍTULO VI – RÉGIMEN DE REPATRIACIÓN**
- **TÍTULO VII – SANCIONES**
- **TÍTULO VIII – COOPERACIÓN INTERNACIONAL**

### **PARTE II**

- **FIRMADOS**

### **PARTE III — ANEXOS COMPLEMENTARIOS**

- **ANEXO I - DEFINICIONES TÉCNICAS Y CRITERIOS OPERATIVOS**
- **ANEXO II - PROCEDIMIENTO DE DECLARACIÓN, AUDITORÍA Y ACTUALIZACIÓN**
- **ANEXO III - SISTEMA DE TRAZABILIDAD Y MAPA NACIONAL DE ACTIVOS ESTRATÉGICOS EXTERNOS**
- **ANEXO IV - PROTOCOLOS DE CRISIS, REPATRIACIÓN Y BLINDAJE ECONÓMICO**
- **ANEXO V - INCENTIVOS, GRADUALIDAD Y REGULARIZACIÓN VOLUNTARIA**

# **PROYECTO DE LEY DE RÉGIMEN DE DECLARACIÓN OBLIGATORIA DE ACTIVOS ESTRATÉGICOS EXTERNOS.**

## **Artículo 1º – Objeto.**

La presente ley tiene por objeto establecer la **declaración obligatoria, trazabilidad, auditoría y supervisión permanente** de todos los activos estratégicos ubicados en el exterior, con el fin de **proteger la estabilidad macroeconómica, garantizar la soberanía financiera, prevenir la fuga de capitales y asegurar el resguardo de los bienes estratégicos de la Nación.**

---

## **TÍTULO I – DEFINICIONES Y SUJETOS OBLIGADOS**

### **Artículo 2º – Activos Estratégicos Externos.**

A los efectos de esta ley, se consideran **activos estratégicos externos** todos aquellos bienes, derechos o recursos ubicados fuera del territorio nacional que pertenezcan a, o sean administrados por:

- a. Empresas con participación estatal mayoritaria o minoritaria, directa o indirecta.
- b. Empresas privadas beneficiarias de subsidios, créditos, avales, exenciones o apoyo financiero del Estado nacional.
- c. Entidades financieras públicas o privadas radicadas en el país.
- d. Bancos, fintech, administradoras de fondos o fiduciarios con operaciones fuera del país vinculadas a actividades reguladas en Argentina.
- e. Personas jurídicas privadas que gestionen recursos públicos, concesiones o bienes estratégicos.
- f. Personas humanas residentes fiscales que sean beneficiarias de subsidios estatales, regímenes promocionales o que operen en sectores definidos como estratégicos.

### **Artículo 2º bis — Principio de función social y soberanía del capital**

La presente ley se interpreta y aplica conforme a los principios constitucionales de **función social de la propiedad, interés económico general, estabilidad**

**macroeconómica y soberanía financiera**, sin perjuicio del derecho de propiedad reconocido por la Constitución Nacional.

Los activos estratégicos, por su impacto sistémico, quedan sujetos a **regímenes especiales de información, control y supervisión**, en resguardo del interés público y del desarrollo nacional.

---

## **TÍTULO II – ALCANCE DE LA DECLARACIÓN OBLIGATORIA**

### **Artículo 3º – Alcance de la declaración.**

Los sujetos obligados deberán declarar, en forma anual y auditada:

- a) Cuentas bancarias, depósitos, inversiones financieras y activos en paraísos fiscales.
  - b) Empresas offshore, sociedades vehículo, holdings o trusts.
  - c) Activos físicos o digitales, incluyendo criptoactivos, pero no limitados a criptoactivos, incluyen patentes, royalties, propiedad intelectual y derechos contractuales.
  - d) Flujos de capital provenientes de actividades en el país y transferidos al exterior.
  - e) Toda estructura societaria internacional que pueda afectar la balanza de pagos, la competitividad o las reservas nacionales.
- 

## **TÍTULO III – INFORMACIÓN ABIERTA Y AUDITABLE**

### **Artículo 4º – Integración con la Ley de Datos Soberanos Abiertos.**

Toda la información declarada deberá incorporarse, en formato **abierto, auditible y trazable**, al Sistema Nacional de Datos Soberanos Abiertos (SINDASA), conforme estándares internacionales de interoperabilidad.

### **Artículo 5º – Clasificación y resguardo.**

El Poder Ejecutivo podrá clasificar información sensible exclusivamente por razones de seguridad económica nacional.

La clasificación no impedirá la **auditoría obligatoria**, ni la disponibilidad de datos agregados para el control ciudadano.

### **Artículo 5º bis — Apertura responsable y protección de información sensible**

La información incorporada al Sistema Nacional de Datos Soberanos Abiertos (SINDASA) en virtud de la presente ley será publicada **en forma agregada, anonimizada y no individualizable**, garantizando:

- a) la protección del secreto bancario y comercial,
- b) la seguridad económica nacional,
- c) la protección de datos personales,
- d) el cumplimiento de tratados internacionales vigentes.

La clasificación de información sensible no impedirá en ningún caso la **auditoría integral por parte de los organismos competentes** ni el control institucional del Estado.

---

## **TÍTULO IV – BANCA PÚBLICA Y PRIVADA COMO INFRAESTRUCTURA ESTRATÉGICA**

### **Artículo 6º – Reconocimiento de la banca como activo estratégico.**

La banca pública y privada que opere en el sistema financiero nacional es declarada **infraestructura estratégica**, en virtud de su rol sistémico, su impacto macroeconómico y su función de intermediación del ahorro nacional, debiendo:

- a. Declarar operaciones transfronterizas.
- b. Informar cuentas espejo, movimientos hacia jurisdicciones de riesgo y estructuras societarias vinculadas.
- c. Proveer trazabilidad sobre flujos en divisas originados en operaciones locales.

### **Artículo 6º bis — Fundamento del carácter estratégico del sistema financiero**

Declarase que el sistema bancario y financiero que opera en la República Argentina constituye **infraestructura económica estratégica**, en virtud de:

- a) su rol sistémico en la intermediación del ahorro nacional,
- b) su impacto directo en la balanza de pagos y las reservas internacionales,
- c) su función en la estabilidad monetaria, crediticia y cambiaria,
- d) su vinculación con recursos públicos, subsidios, avales y regulaciones estatales.

En consecuencia, queda sujeto a los deberes reforzados de información y trazabilidad establecidos en la presente ley.

---

# **TÍTULO V – RÉGIMEN DE REINVERSIÓN Y LIQUIDACIÓN MÍNIMA**

## **Artículo 7º – Reinversión interna obligatoria.**

Las empresas reguladas por esta ley deberán mantener un **mínimo del 30%** de su excedente financiero anual en inversiones productivas internas certificadas.

## **Artículo 7º bis — Gradualidad y razonabilidad en la aplicación**

**Las obligaciones de reinversión interna y liquidación mínima de divisas previstas en los artículos 7º y 8º podrán aplicarse de manera progresiva durante los primeros tres (3) ejercicios fiscales, conforme a la reglamentación, atendiendo a:**

- a) la situación macroeconómica general,
- b) el sector de actividad,
- c) el tamaño del sujeto obligado,
- d) la preservación del empleo y la capacidad productiva.

La gradualidad no podrá implicar exenciones permanentes ni vaciamiento del objetivo de la ley.

## **Artículo 8º – Liquidación obligatoria de divisas.**

Los sujetos alcanzados deberán liquidar en el sistema financiero argentino **al menos el 40%** de sus ingresos en moneda extranjera generados a partir de actividades económicas que dependan del mercado interno.

---

# **TÍTULO VI – RÉGIMEN DE REPATRIACIÓN**

## **Artículo 9º – Repatriación obligatoria excepcional.**

En caso de crisis cambiaria, riesgo de hiperinflación, estrés de reservas o fuga sistemática, el Poder Ejecutivo podrá exigir la **repatriación del 20%** de los activos estratégicos externos declarados, previo dictamen técnico fundado del Banco Central y del Ministerio de Economía.

## **Artículo 9º bis — Condiciones objetivas para la repatriación excepcional**

**Las medidas de repatriación obligatoria previstas en el artículo 9º solo podrán adoptarse:**

- a) mediante acto fundado del Poder Ejecutivo,
- b) previo dictamen técnico del Banco Central de la República Argentina y del Ministerio de Economía,
- c) con determinación expresa de la causal macroeconómica habilitante,
- d) por tiempo determinado y proporcional a la situación que las motiva.

Toda medida deberá ser comunicada al Congreso de la Nación.

**Artículo 10º – Repatriación para activos ocultos o no declarados.**

Cuando se verifique la existencia de activos no declarados, el sujeto obligado deberá repatriar **hasta el 60%** del total no registrado y quedará inhabilitado para recibir subsidios o contratos estatales por diez años.

---

## **TÍTULO VII – SANCIONES**

**Artículo 11º – Sanciones administrativas.**

Incluyen:

- a) Multas de hasta cinco veces el valor del activo no declarado.
- b) Suspensión de licencias, beneficios fiscales y concesiones.
- c) Inhabilitación permanente para operar con el Estado.

**Artículo 12º – Sanciones penales.**

La ocultación dolosa de activos estratégicos externos será penada como **evasión agravada, fraude al Estado y atentado contra la estabilidad económica nacional** sin perjuicio de las sanciones penales previstas en el Código Penal y leyes especiales.

---

## **TÍTULO VIII – COOPERACIÓN INTERNACIONAL**

**Artículo 13º – Jurisdicciones de riesgo.**

El Poder Ejecutivo publicará anualmente el **Mapa Nacional de Activos Externos**, que identificará:

- a) Jurisdicciones utilizadas para ocultamiento o evasión.
- b) Listado de empresas o estructuras que deban repatriar capital.
- c) Reportes de riesgo para organismos multilaterales.

**Artículo 14º – Convenios globales.**

La autoridad de aplicación gestionará la adhesión a FATF-GAFI, CRS-OECD, UNSIF,

ESRB y sistemas internacionales de intercambio automático de información en tiempo real.

#### **Artículo 14° bis — Articulación con regímenes de transparencia y promoción**

El cumplimiento de la presente ley será **condición necesaria** para:

- a) acceder a regímenes de promoción de inversiones, incluyendo el RIGI y sus ampliaciones,
- b) recibir subsidios, beneficios fiscales, avales o créditos públicos,
- c) contratar con el Estado nacional.

La información recabada se articulará con la **Ley de Transparencia y Beneficiarios Reales** y la **Ley de Datos Abiertos Soberanos**, respetando los principios de coherencia normativa y soberanía de datos.

#### **Artículo 16° – Blindaje en Caso de Crisis Económica**

En situaciones de crisis cambiaria, inestabilidad económica o hiperinflación, el Poder Ejecutivo podrá aplicar medidas excepcionales para garantizar la soberanía financiera. Estas medidas incluyen:

- a) Requiere la repatriación obligatoria de activos estratégicos.
- b) Restricciones adicionales en los flujos de divisas hacia paraísos fiscales y jurisdicciones no cooperativas.
- c) Suspensión temporal de beneficios fiscales para aquellos sujetos obligados que no cumplan con la repatriación de activos.

#### **Artículo 17° – Articulación con el Sistema Financiero Nacional**

Se establece un sistema interinstitucional de monitoreo y control de activos estratégicos en el exterior, compuesto por:

- a) **Banco Central de la República Argentina (BCRA)**: Para monitorear el impacto de la repatriación en las reservas nacionales y en el sistema financiero.
- b) **Administración Federal de Ingresos Públicos (AFIP)**: Para coordinar las auditorías y supervisar el cumplimiento de las declaraciones y repatriaciones.
- c) **Ministerio de Economía**: Para la planificación y ejecución de las políticas económicas vinculadas a la ley.

#### **Artículo 18° – Coordinación Internacional**

La República Argentina adoptará acuerdos bilaterales y multilaterales con países miembros de organismos internacionales, como el **FATF-GAFI, OCDE y Grupo de Acción Financiera Internacional**, para mejorar la trazabilidad de los activos, fomentar la cooperación y garantizar el cumplimiento de los estándares internacionales de transparencia financiera.

#### **Artículo 19° – Medidas de Blindaje en el Caso de Activos No Declarados**

En caso de detectar activos no declarados, se podrá aplicar:

- a) La inhabilitación para acceder a nuevos subsidios o contratos estatales.
- b) La repatriación obligatoria de hasta el 60% de dichos activos.
- c) Multas que podrán alcanzar hasta cinco veces el valor del activo no declarado.

**Artículo 20º – Acuerdos de Protección de Datos**

Se firmarán acuerdos con países y organizaciones internacionales para asegurar el respeto por la soberanía de los datos nacionales y la protección de la información económica sensible.

---

**Artículo 21º – Entrada en vigencia.**

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

**Firmado:**  
**Natividad Vidal**  
Autora del Proyecto  
Capilla del Monte, Córdoba, Argentina

**Firma manuscrita digital:**



Natividad Vidal  
DNI 27.716.481

**Correo institucional:**  
[datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

**Acreditación:**  
El presente proyecto es presentado en carácter de autora ciudadana y en cumplimiento de estándares internacionales de Gobierno Abierto, Transparencia Digital y Soberanía de Datos.

# **ANEXO I - DEFINICIONES TÉCNICAS Y CRITERIOS OPERATIVOS**

---

## **Activo estratégico externo**

Se considera **activo estratégico externo** todo bien, derecho, instrumento financiero, activo físico o digital, recurso intangible o estructura jurídica ubicada fuera del territorio nacional que:

- a) tenga incidencia directa o indirecta en la balanza de pagos,
- b) derive total o parcialmente de actividades económicas realizadas en la República Argentina,
- c) esté vinculado a sectores estratégicos definidos por el Estado nacional,
- d) sea susceptible de afectar la estabilidad macroeconómica, financiera o cambiaria.

Incluye, sin carácter taxativo:

- cuentas bancarias y financieras,
  - inversiones directas o de cartera,
  - sociedades offshore, holdings, trusts y fundaciones,
  - criptoactivos y tokens,
  - patentes, marcas, royalties y licencias,
  - derechos contractuales con contraparte extranjera.
- 

## **Activos estratégicos por sector**

Se consideran sectores estratégicos, entre otros:

- a) energía, minería y recursos naturales,
- b) alimentos, agua y biodiversidad,
- c) infraestructura crítica y logística,
- d) sistema financiero y asegurador,
- e) telecomunicaciones, datos y tecnología digital,
- f) defensa, salud y medicamentos esenciales.

La autoridad de aplicación podrá actualizar el listado mediante resolución fundada.

---

## **Jurisdicciones de riesgo**

Se entiende por **jurisdicción de riesgo** toda aquella que:

- a) no coopere con sistemas automáticos de intercambio de información,
- b) presente regímenes de secreto financiero o societario reforzado,
- c) facilite la evasión fiscal, el lavado de activos o la opacidad corporativa,
- d) sea identificada como tal por organismos internacionales o por la autoridad de aplicación.

La clasificación será pública y revisable anualmente.

---

## **Sujeto obligado**

A los efectos del presente régimen, se considera **sujeto obligado** toda persona humana o jurídica que:

- a) sea residente fiscal en la República Argentina,
- b) reciba subsidios, beneficios fiscales o contratos públicos,
- c) opere en sectores estratégicos,
- d) administre recursos públicos o concesiones,
- e) integre cadenas financieras o corporativas transnacionales con impacto local.

---

## **Beneficiario real (articulación)**

Se considera **beneficiario real** a la persona humana que, directa o indirectamente:

- a) posea, controle o se beneficie económicamente de un activo estratégico externo,
- b) ejerza influencia decisiva sobre su administración,
- c) reciba rendimientos, dividendos o derechos económicos sustanciales.

La identificación del beneficiario real se realizará conforme a la Ley de Transparencia y Beneficiarios Reales.

---

## **Principio de trazabilidad integral**

Toda declaración deberá permitir reconstruir:

- a. el origen económico del activo,
- b) su circuito de transferencia,
- c) su titularidad real,
- d) su vinculación con actividades desarrolladas en el país.

# **ANEXO II - PROCEDIMIENTO DE DECLARACIÓN, AUDITORÍA Y ACTUALIZACIÓN**

---

## **Sistema único de declaración**

La declaración de activos estratégicos externos se realizará a través de un **Sistema Único de Declaración de Activos Estratégicos Externos (SUDAEE)**, administrado por la autoridad de aplicación, interoperable con:

- a) el Banco Central de la República Argentina,
- b) la autoridad tributaria nacional,
- c) la Unidad de Información Financiera,
- d) el Sistema Nacional de Datos Soberanos Abiertos (SINDASA).

El sistema garantizará trazabilidad, integridad, seguridad y auditabilidad de la información.

---

## **Contenido mínimo de la declaración**

Cada sujeto obligado deberá declarar, como mínimo:

- a) identificación del activo y su naturaleza jurídica,
  - b) jurisdicción de radicación,
  - c) valuación económica conforme normas vigentes,
  - d) origen de los fondos o recursos que dieron lugar al activo,
  - e) estructura societaria asociada,
  - f) identificación del beneficiario real,
  - g) flujos económicos generados durante el período declarado.
- 

## **Periodicidad y actualización**

La declaración será:

- a) **anual**, dentro de los plazos que establezca la reglamentación,
- b) **actualizada** cuando se produzcan:
  - modificaciones sustanciales en la titularidad,
  - transferencias relevantes,
  - cambios de jurisdicción,
  - creación o disolución de estructuras asociadas.

La omisión de actualización será considerada incumplimiento.

---

### **Valuación de activos**

La valuación deberá realizarse conforme a:

- a) normas contables nacionales e internacionales aplicables,
- b) criterios de mercado verificables,
- c) metodologías específicas para activos intangibles y digitales.

La autoridad de aplicación podrá requerir revaluaciones cuando existan indicios fundados de subdeclaración.

---

### **Auditoría obligatoria**

Toda declaración estará sujeta a **auditoría técnica obligatoria**, que podrá ser:

- a) interna, por organismos estatales competentes,
- b) externa, mediante auditores registrados y habilitados,
- c) cruzada, mediante intercambio automático de información.

Las auditorías deberán preservar el debido proceso y el derecho de defensa.

---

### **Cruce de información y alertas tempranas**

El sistema implementará mecanismos automáticos de:

- a) detección de inconsistencias,
  - b) identificación de jurisdicciones de riesgo,
  - c) alertas por flujos atípicos o desvíos significativos,
  - d) cruces con regímenes de beneficiario real y transparencia fiscal.
- 

### **Rectificación voluntaria**

Los sujetos obligados podrán realizar **rectificaciones voluntarias** dentro de los plazos reglamentarios, sin perjuicio de:

- a) la obligación de regularizar la situación,
- b) la aplicación de sanciones reducidas cuando corresponda.

La rectificación no extingue responsabilidades en caso de ocultamiento doloso.

---

### **Conservación de la información**

La información declarada deberá conservarse por un plazo mínimo de **diez (10) años**, en soportes digitales seguros, garantizando:

- a) integridad,
  - b) disponibilidad,
  - c) trazabilidad histórica.
- 

#### **Acceso institucional a la información**

Tendrán acceso pleno a la información individualizada:

- a) la autoridad de aplicación,
- b) el Banco Central,
- c) la autoridad tributaria,
- d) la UIF,
- e) el Poder Judicial, mediante orden fundada.

El acceso ciudadano se realizará conforme a lo establecido en el artículo 5° bis de la ley.

## **ANEXO III - SISTEMA DE TRAZABILIDAD Y MAPA NACIONAL DE ACTIVOS ESTRATÉGICOS EXTERNOS**

#### **Sistema Nacional de Trazabilidad de Activos Externos**

Créase el **Sistema Nacional de Trazabilidad de Activos Estratégicos Externos (SINTAEE)** como subsistema del Sistema Nacional de Datos Soberanos Abiertos (SINDASA), con el objeto de:

- a) registrar y vincular las declaraciones de activos estratégicos externos,
- b) garantizar trazabilidad histórica y verificabilidad,
- c) facilitar auditorías técnicas e institucionales,
- d) generar información agregada para la formulación de políticas públicas.

El sistema operará bajo principios de **soberanía de datos, seguridad, integridad y transparencia responsable**.

---

#### **Registro y encadenamiento de información**

Cada activo declarado será identificado mediante:

- a) un identificador único no reutilizable,
- b) metadatos normalizados,

- c) registro de modificaciones, transferencias y eventos relevantes,
- d) vinculación con el beneficiario real correspondiente.

Los registros no podrán ser alterados sin dejar trazabilidad completa de los cambios.

---

### **Tecnologías de registro y verificación**

El sistema podrá utilizar tecnologías de:

- a) registros distribuidos,
- b) sellado temporal,
- c) hash criptográfico,
- d) tokenización de información representativa no transferible,

exclusivamente con fines de **verificación, integridad y auditoría**, quedando prohibido su uso especulativo o comercial.

Articulación directa con la Ley de Tokenización Ética.

---

### **Mapa Nacional de Activos Estratégicos Externos**

Créase el **Mapa Nacional de Activos Estratégicos Externos**, como herramienta de análisis público e institucional, que contendrá:

- a) distribución geográfica agregada de activos,
- b) sectores económicos involucrados,
- c) jurisdicciones de riesgo,
- d) niveles de concentración y exposición sistémica.

El mapa no contendrá información individualizable.

---

### **Actualización y periodicidad**

El Mapa Nacional será:

- a) actualizado como mínimo una vez por año,
  - b) revisado ante eventos macroeconómicos relevantes,
  - c) utilizado como insumo para informes al Congreso y organismos internacionales.
- 

### **Alertas sistémicas y análisis de riesgo**

El sistema generará indicadores de:

- a) concentración excesiva de activos en determinadas jurisdicciones,
- b) desvíos significativos de flujos financieros,
- c) riesgos de fuga sistémica,
- d) exposición macroeconómica sectorial.

Las alertas tendrán carácter preventivo y no sancionatorio por sí mismas.

---

### **Acceso a la información**

El acceso al sistema se regirá por los siguientes niveles:

- a) acceso pleno institucional para organismos competentes,
  - b) acceso agregado y anonimizado para la ciudadanía,
  - c) acceso restringido para información clasificada por seguridad económica.
- 

### **Cooperación interinstitucional e internacional**

El sistema será interoperable con:

- a) sistemas nacionales de control financiero,
- b) plataformas de intercambio automático de información,
- c) organismos multilaterales, conforme tratados vigentes.

Toda cooperación respetará la soberanía de los datos nacionales.

## **ANEXO IV - PROTOCOLOS DE CRISIS, REPATRIACIÓN Y BLINDAJE ECONÓMICO**

### **Definición de evento de riesgo macroeconómico**

A los efectos de la presente ley, se consideran **eventos de riesgo macroeconómico** aquellos en los que se verifique, de manera concurrente o alternativa:

- a) caída significativa y sostenida de reservas internacionales,
- b) estrés cambiario severo o pérdida abrupta de valor de la moneda,
- c) interrupción del financiamiento externo esencial,
- d) fuga sistemática de capitales,
- e) riesgo cierto de hiperinflación o desabastecimiento crítico.

La declaración del evento deberá ser fundada técnicamente.

---

### **Procedimiento de activación del protocolo**

El **Protocolo de Crisis y Repatriación** se activará únicamente mediante:

- a) informe técnico del Banco Central de la República Argentina,
- b) dictamen del Ministerio de Economía,
- c) acto administrativo fundado del Poder Ejecutivo,
- d) comunicación inmediata al Congreso de la Nación.

La activación deberá establecer alcance, duración y objetivos.

---

### **Medidas excepcionales habilitadas**

Durante la vigencia del protocolo, el Poder Ejecutivo podrá disponer, de forma proporcional y temporal:

- a) repatriación obligatoria parcial de activos estratégicos externos,
- b) priorización de liquidación de divisas en el mercado local,
- c) restricciones transitorias a operaciones hacia jurisdicciones de riesgo,
- d) suspensión temporal de beneficios fiscales o regímenes promocionales.

En ningún caso las medidas podrán implicar confiscación.

---

### **Criterios de proporcionalidad y temporalidad**

Las medidas adoptadas deberán:

- a) ser necesarias para superar el evento de riesgo,
- b) aplicarse por tiempo determinado,
- c) afectar en forma razonable y no discriminatoria a los sujetos obligados,
- d) revisarse periódicamente.

Toda prórroga requerirá nueva fundamentación técnica.

---

### **Protección del empleo y la producción**

La aplicación del protocolo deberá preservar:

- a) la continuidad de actividades productivas esenciales,
- b) el empleo formal,
- c) las cadenas de valor estratégicas.

La reglamentación establecerá mecanismos de adecuación sectorial.

---

### **Seguimiento y control institucional**

Durante la vigencia del protocolo:

- a) el Congreso recibirá informes periódicos,
- b) los organismos de control ejercerán auditoría reforzada,
- c) se publicará información agregada sobre resultados e impacto.

---

### **Cese del protocolo**

El protocolo cesará automáticamente cuando:

- a) desaparezcan las condiciones que lo motivaron,
- b) se alcance el objetivo macroeconómico definido,
- c) venza el plazo máximo establecido en el acto de activación.

El cese será comunicado formalmente al Congreso.

---

## **ANEXO V - INCENTIVOS, GRADUALIDAD Y REGULARIZACIÓN VOLUNTARIA**

### **Principio de incentivo al cumplimiento**

El régimen establecido por la presente ley se rige por el **principio de incentivo al cumplimiento voluntario**, priorizando:

- a) la regularización temprana de activos,
- b) la transparencia patrimonial,
- c) la repatriación productiva,
- d) la estabilidad macroeconómica.

Las sanciones tendrán carácter **subsidiario** frente al incumplimiento doloso o reiterado.

---

### **Regularización voluntaria inicial**

Dentro de los **doce (12) meses** desde la entrada en vigencia de la ley, los sujetos obligados podrán acceder a un **Régimen de Regularización Voluntaria Inicial**, que permitirá:

- a) declarar activos no registrados,
- b) corregir valuaciones subdeclaradas,
- c) transparentar estructuras societarias complejas,
- d) identificar beneficiarios reales.

La adhesión al régimen no implicará reconocimiento automático de delito.

---

### **Beneficios por adhesión temprana**

Los sujetos que adhieran al régimen de regularización voluntaria podrán acceder, conforme reglamentación, a:

- a) reducción de sanciones administrativas,
- b) exclusión de inhabilitaciones temporales,
- c) prioridad en programas de inversión productiva,
- d) acceso a líneas de financiamiento para reinversión interna.

No se aplicará este beneficio en casos de fraude agravado o activos vinculados a delitos penales graves.

---

### **Repatriación productiva incentivada**

La repatriación voluntaria de activos estratégicos externos podrá ser aplicada a:

- a) inversión productiva nacional,
- b) infraestructura estratégica,
- c) economía del conocimiento,
- d) transición energética y tecnológica.

La reglamentación establecerá mecanismos de certificación del destino productivo.

---

### **Gradualidad según perfil del sujeto obligado**

La autoridad de aplicación podrá establecer **esquemas de adecuación gradual**, considerando:

- a) tamaño del sujeto obligado,
- b) sector de actividad,
- c) nivel de complejidad de los activos,
- d) impacto macroeconómico.

La gradualidad no podrá utilizarse para eludir el cumplimiento sustantivo.

---

### **Tratamiento diferencial para economías regionales**

Se contemplará un tratamiento diferenciado para:

- a) pequeñas y medianas empresas,
- b) cooperativas y economía social,
- c) economías regionales estratégicas,

priorizando asistencia técnica y acompañamiento institucional.

---

### **Exclusión de beneficios**

Quedarán excluidos de los beneficios del presente anexo:

- 
- a) sujetos con reincidencia dolosa,
  - b) activos vinculados a lavado de dinero, financiamiento del terrorismo u otros delitos graves,
  - c) estructuras creadas exclusivamente para el ocultamiento patrimonial.
- 

#### **Coordinación interinstitucional**

La implementación del presente anexo se coordinará con:

- a) la autoridad tributaria nacional,
  - b) el Banco Central,
  - c) la Unidad de Información Financiera,
  - d) los organismos de control competentes.
- 

#### **Principio de cierre del régimen excepcional**

El régimen de regularización voluntaria tendrá carácter **excepcional y transitorio**.

Vencido el plazo establecido, se aplicará plenamente el régimen sancionatorio previsto en la ley

# **PROYECTO DE LEY**

## **Ampliacion del Regimen de Incentivo para Grandes Inversiones (RIGI) y Creacion del Fondo Nacional de Renta Tecnologica y Social (FONARETS) – ARGENTINA 2025**

### **Autora:**

Natividad Vidal

Capilla del Monte, Córdoba, Argentina

**Correo Institucional:** [datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

### **Presentado ante:**

Honorable Cámara de Diputados de la Nación

Honorable Cámara de Senadores de la Nación

**Fecha:** \_\_\_\_\_ (colocar al momento de presentación)



Natividad Vidal

DNI 27.716.481

Proyecto presentado para su tratamiento en el marco del Programa de Soberanía Digital Argentina, alineado con estándares ONU – CEPAL – OGP.

## **INDICE GENERAL**

### **PARTE I — TEXTO DEL PROYECTO DE LEY**

- **TÍTULO I – DISPOSICIONES GENERALES**
- **TÍTULO II – ALCANCE Y CONDICIONALIDADES**
- **TÍTULO III – FONDO NACIONAL DE RENTA TECNOLÓGICA Y SOCIAL**
- **TÍTULO IV – CANON TERRITORIAL Y RENTA LOCAL**
- **TÍTULO V – DATOS, ÉTICA DIGITAL Y SOBERANÍA TECNOLÓGICA**
- **TÍTULO VI – CONTROL, EVALUACIÓN Y SUPERVISIÓN**
- **TÍTULO VII – BENEFICIOS Y PÉRDIDA DE BENEFICIOS**
- **TÍTULO VIII – FEDERALIZACIÓN PRODUCTIVA**
- **TÍTULO IX – DISPOSICIONES FINALES**
- **FUNDAMENTOS**

### **PARTE II**

- **FIRMADOS**

### **PARTE III — ANEXOS COMPLEMENTARIOS**

- **ANEXO I - CRITERIOS ESG OBLIGATORIOS PARA PROYECTOS RIGI**
- **ANEXO II - METODOLOGÍA DE CÁLCULO Y ADMINISTRACIÓN DEL FONARETS**
- **ANEXO III - ESTÁNDARES DE TRANSFERENCIA TECNOLÓGICA**
- **ANEXO IV - DATOS ABIERTOS, AUDITORÍA Y TRANSPARENCIA**
- **ANEXO V - RÉGIMEN TRANSITORIO, ADECUACIÓN Y SALIDA ORDENADA**

# **PROYECTO DE LEY**

## **AMPLIACIÓN DEL RÉGIMEN DE INCENTIVO PARA GRANDES INVERSIONES (RIGI)**

## **Y CREACIÓN DEL FONDO NACIONAL DE RENTA TECNOLÓGICA Y SOCIAL (FONARETS)**

---

### **TÍTULO I – DISPOSICIONES GENERALES**

#### **Artículo 1º – Objeto**

Créase la Ampliación del Régimen de Incentivo para Grandes Inversiones (RIGI Ampliado), incorporando criterios obligatorios de **sostenibilidad, transparencia patrimonial, soberanía tecnológica y renta social**, y créase el **Fondo Nacional de Renta Tecnológica y Social (FONARETS)**.

---

#### **Artículo 2º – Principios rectores**

El régimen se regirá por los siguientes principios obligatorios:

- a) previsibilidad jurídica,
  - b) sostenibilidad ambiental y tecnológica,
  - c) transparencia y beneficiarios reales,
  - d) contrapartida productiva nacional,
  - e) renta social y territorial,
  - f) desarrollo federal,
  - g) innovación responsable.
-

## **TÍTULO II – ALCANCE Y CONDICIONALIDADES**

### **Artículo 3º – Condición habilitante**

El acceso y permanencia en el RIGI Ampliado estará condicionado al **cumplimiento simultáneo** de:

- a) Ley de Transparencia y Registro de Beneficiarios Reales,
- b) Ley de Declaración Obligatoria de Activos Estratégicos Externos,
- c) Ley de Datos Abiertos Soberanos,
- d) normativa ambiental y de sostenibilidad tecnológica.

El incumplimiento de cualquiera de estas normas implicará la **suspensión automática de beneficios**.

---

### **Artículo 4º – Contrapartida Nacional Productiva**

Toda inversión RIGI deberá incluir obligatoriamente:

- a) un mínimo del **30 % de proveedores locales**,
  - b) programas de **formación laboral certificada**,
  - c) transferencia tecnológica verificable,
  - d) participación de universidades o centros científicos nacionales.
- 

## **TÍTULO III – FONDO NACIONAL DE RENTA TECNOLÓGICA Y SOCIAL**

### **Artículo 5º – Creación del FONARETS**

Créase el **Fondo Nacional de Renta Tecnológica y Social (FONARETS)**, destinado a:

- a) pensiones y protección social,
  - b) alfabetización digital y tecnológica,
  - c) ciencia aplicada e innovación productiva,
  - d) infraestructura tecnológica pública.
-

## **Artículo 6º – Financiamiento**

El FONARETS se financiará con:

- a) un aporte obligatorio de entre el **1,5 % y el 3 %** de las utilidades netas del proyecto RIGI,
  - b) cánones territoriales,
  - c) multas y sanciones,
  - d) aportes internacionales.
- 

## **TÍTULO IV – CANON TERRITORIAL Y RENTA LOCAL**

### **Artículo 7º – Canon local y regalías sociales**

Los proyectos que utilicen recursos naturales, energéticos o territoriales deberán abonar un **canon local**, distribuido de la siguiente forma:

- a) 40 % a gobiernos provinciales y municipales,
  - b) 30 % a fondos comunitarios y territoriales,
  - c) 30 % a proyectos de desarrollo local y ambiental.
- 

## **TÍTULO V – DATOS, ÉTICA DIGITAL Y SOBERANÍA TECNOLÓGICA**

### **Artículo 8º – Integración con Datos Abiertos**

Las empresas RIGI deberán:

- a) publicar información agregada y no sensible,
  - b) cumplir estándares de ética digital,
  - c) garantizar soberanía y trazabilidad tecnológica,
  - d) permitir auditoría estatal y ciudadana.
-

# **TÍTULO VI – CONTROL, EVALUACIÓN Y SUPERVISIÓN**

## **Artículo 9° – Evaluación escalonada**

Los proyectos se implementarán por fases obligatorias, con evaluaciones de:

- a) impacto económico,
  - b) impacto social,
  - c) impacto ambiental,
  - d) cumplimiento de contrapartidas.
- 

## **Artículo 10° – Órgano de supervisión**

Créase la **Mesa Nacional de Transición Digital Justa y Desarrollo Federal**, integrada por:

- Estado nacional,
  - provincias,
  - universidades,
  - organismos técnicos independientes.
- 

# **TÍTULO VII – BENEFICIOS Y PÉRDIDA DE BENEFICIOS**

## **Artículo 11° – Beneficios estratégicos**

El régimen otorgará:

- a) estabilidad regulatoria condicionada,
  - b) reputación ESG certificada,
  - c) acceso preferente a infraestructura estratégica.
- 

## **Artículo 12° – Pérdida de beneficios**

La falsedad, ocultamiento patrimonial, incumplimiento ambiental o evasión implicarán:

- 
- a) pérdida inmediata de beneficios,
  - b) devolución de incentivos recibidos,
  - c) inhabilitación para futuros regímenes.
- 

## **TÍTULO VIII – FEDERALIZACIÓN PRODUCTIVA**

### **Artículo 13° – Polos federales**

Se promoverá la creación de **polos tecnológicos, energéticos y productivos federales**, priorizando regiones con menor desarrollo relativo.

---

## **TÍTULO IX – DISPOSICIONES FINALES**

### **Artículo 14° – Reglamentación**

El Poder Ejecutivo reglamentará la presente ley en un plazo máximo de **120 días**.

---

### **Artículo 15° – Informe de impacto**

A los **24 meses** de su implementación se presentará un informe público integral de resultados.

---

### **Artículo 16° – Comuníquese**

Comuníquese al Poder Ejecutivo Nacional.

**Firmado:**

**Natividad Vidal**

Autora del Proyecto

Capilla del Monte, Córdoba, Argentina

**Firma manuscrita digital:**



Natividad Vidal

DNI 27.716.481

**Correo institucional:**

datosabiertossoberanosar@gmail.com

**Acreditación:**

El presente proyecto es presentado en carácter de autora ciudadana y en cumplimiento de estándares internacionales de Gobierno Abierto, Transparencia Digital y Soberanía de Datos.

# **ANEXO I - CRITERIOS ESG OBLIGATORIOS PARA PROYECTOS RIGI**

## **Alcance**

Todo proyecto aprobado bajo el RIGI Ampliado deberá cumplir criterios **ESG mínimos verificables** (Ambientales, Sociales y de Gobernanza).

---

## **Criterios Ambientales**

Los proyectos deberán acreditar:

- a) uso progresivo de **energías renovables** (mínimo 40 % inicial, 80 % a 5 años),
  - b) eficiencia energética certificada,
  - c) gestión responsable del agua y residuos,
  - d) evaluación de impacto ambiental acumulativo,
  - e) planes de mitigación y remediación.
- 

## **Criterios Sociales**

Deberán incluir:

- a) generación de empleo local registrado,
  - b) programas de capacitación laboral,
  - c) respeto a comunidades locales y pueblos originarios,
  - d) mecanismos de participación comunitaria.
- 

## **Criterios de Gobernanza**

Será obligatorio:

- a) identificación de beneficiarios reales,
- b) publicación de información agregada del proyecto,

- 
- c) auditorías externas periódicas,
  - d) cumplimiento anticorrupción y antilavado.
- 

## **ANEXO II - METODOLOGÍA DE CÁLCULO Y ADMINISTRACIÓN DEL FONARETS**

### **Base de cálculo**

El aporte al FONARETS se calculará sobre:

- utilidades netas auditadas,
  - rentas extraordinarias,
  - beneficios fiscales efectivamente percibidos.
- 

### **Alícuotas**

El aporte será progresivo:

- 1,5 % para proyectos de bajo impacto,
  - hasta 3 % para proyectos intensivos en recursos estratégicos.
- 

### **Administración**

El Fondo será administrado por un órgano fiduciario público, con:

- cuentas separadas,
  - trazabilidad digital,
  - publicación anual de resultados.
- 

## **ANEXO III - ESTÁNDARES DE TRANSFERENCIA TECNOLÓGICA**

## **Obligación mínima**

Todo proyecto deberá presentar un **Plan de Transferencia Tecnológica**, que incluya:

- a) capacitación técnica local,
  - b) acceso a conocimiento operativo,
  - c) cooperación con universidades y centros científicos.
- 

## **Indicadores verificables**

La transferencia se evaluará mediante:

- número de técnicos formados,
  - tecnologías adaptadas localmente,
  - patentes compartidas o licencias,
  - continuidad del conocimiento tras el proyecto.
- 

# **ANEXO IV - DATOS ABIERTOS, AUDITORÍA Y TRANSPARENCIA**

## **Publicación de información**

Las empresas RIGI deberán publicar, en formato abierto:

- a) estado del proyecto,
  - b) cumplimiento de metas,
  - c) impacto económico, social y ambiental,
  - d) aportes al FONARETS.
- 

## **Auditoría**

Los proyectos estarán sujetos a:

- auditoría estatal,
  - auditoría independiente,
  - control ciudadano mediante datos abiertos.
-

## **Protección de información sensible**

Se resguardará exclusivamente:

- secretos industriales,
- información estratégica crítica.

Nunca se ocultarán beneficiarios reales ni impactos.

---

# **ANEXO V - RÉGIMEN TRANSITORIO, ADECUACIÓN Y SALIDA ORDENADA**

## **Adecuación progresiva**

Los proyectos existentes contarán con **plazos de adecuación** razonables para cumplir los nuevos requisitos.

---

## **Incumplimiento**

El incumplimiento reiterado implicará:

- a) suspensión de beneficios,
  - b) devolución proporcional de incentivos,
  - c) exclusión del régimen.
- 

## **Salida ordenada**

Ante finalización o retiro del proyecto, deberá garantizarse:

- continuidad laboral básica,
- remediación ambiental,
- transferencia de activos estratégicos según corresponda.

# **PROYECTO DE LEY**

## **Renta Basica Tecnologica y Transicion Digital**

### **Sostenible de Argentina – 2025**

#### **Autora:**

Natividad Vidal

Capilla del Monte, Córdoba, Argentina

**Correo Institucional:** [datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

#### **Presentado ante:**

Honorable Cámara de Diputados de la Nación

Honorable Cámara de Senadores de la Nación

**Fecha:** \_\_\_\_\_ (colocar al momento de presentación)



Natividad Vidal

DNI 27.716.481

Proyecto presentado para su tratamiento en el marco del Programa de Soberanía Digital Argentina, alineado con estándares ONU – CEPAL – OGP.

## **PARTE I**

- **TÍTULO I – DISPOSICIONES GENERALES**
- **TÍTULO II – FONDO NACIONAL DE TRANSICIÓN DIGITAL Y RENTA BÁSICA TECNOLÓGICA**
- **TÍTULO III – FUENTES DE FINANCIAMIENTO Y SOBERANÍA**
- **TÍTULO IV – SOSTENIBILIDAD AMBIENTAL Y ENERGÉTICA**
- **TÍTULO V – CONVERGENCIA INTERNACIONAL E INNOVACIÓN**
- **TÍTULO VI – BENEFICIARIOS, ALCANCE Y GRADUALIDAD**
- **TÍTULO VII – MONTO, MODALIDAD Y ACTUALIZACIÓN**
- **TÍTULO VIII – GOBERNANZA Y AUTORIDAD DE APLICACIÓN**
- **TÍTULO IX – TRANSPARENCIA, CONTROL Y EVALUACIÓN**
- **TÍTULO X – ARTICULACIÓN CON EL PAQUETE NORMATIVO**
- **TÍTULO XI – DISPOSICIONES FINALES**
- **FUNDAMENTOS**

## **PARTE II**

- **FIRMADOS**

## **PARTE III**

- **ANEXO I - INDICADORES DE AUTOMATIZACIÓN Y DESPLAZAMIENTO LABORAL**
- **ANEXO II - METODOLOGÍA DE FINANCIAMIENTO DE LA RENTA BÁSICA TECNOLÓGICA**
- **ANEXO III - CANASTA DIGITAL BÁSICA**
- **ANEXO IV - ARTICULACIÓN CON EMPLEO, FORMACIÓN Y TRANSICIÓN LABORAL**
- **ANEXO V - RÉGIMEN PILOTO, GRADUALIDAD Y EVALUACIÓN**

# **PROYECTO DE LEY RENTA BASICA TECNOLOGICA Y TRANSICION DIGITAL SOSTENIBLE**

## **TÍTULO I – DISPOSICIONES GENERALES**

**Artículo 1º – Objeto.** La presente ley tiene por objeto establecer la creación de un régimen de Renta Básica Tecnológica (RBT) como instrumento de inclusión económica y transición digital sostenible, garantizando el acceso universal a los beneficios del progreso tecnológico y la redistribución equitativa de la riqueza generada por la automatización, la inteligencia artificial y el capital digital.

**Artículo 2º – Principios.** La implementación de la presente ley se regirá por los principios de soberanía tecnológica, justicia social, sostenibilidad ambiental, equilibrio fiscal, transparencia, y equidad intergeneracional.

## **TÍTULO II – FONDO NACIONAL DE TRANSICIÓN DIGITAL Y RENTA BÁSICA TECNOLÓGICA**

**Artículo 3º –** Créase el Fondo Nacional de Transición Digital y Renta Básica Tecnológica, destinado a financiar políticas de inclusión y reconversión laboral derivadas de la automatización y la inteligencia artificial, y a garantizar un ingreso básico tecnológico universal.

**Artículo 4º –** El Fondo se constituirá principalmente mediante contribuciones fiscales aplicadas al capital, los beneficios extraordinarios del sector tecnológico, y los rendimientos derivados del uso comercial de datos, evitando la carga tributaria sobre el trabajo humano.

## **TÍTULO III – FUENTES DE FINANCIAMIENTO Y SOBERANÍA**

**Artículo 5°** – La Renta Básica Tecnológica se financiará prioritariamente con recursos nacionales, incluyendo el capital del sector tecnológico, fondos públicos y contribuciones fiscales específicas.

**Artículo 6°** – Se autoriza la recepción de aportes internacionales o privados, siempre que no superen conjuntamente el treinta por ciento (30%) del financiamiento total anual y no impliquen condicionamientos sobre la administración, diseño o distribución del programa, garantizando la soberanía plena del Estado.

**Artículo 7°** – La administración y fiscalización de dichos aportes estará bajo supervisión pública, asegurando transparencia, diversificación de fuentes y publicación de informes anuales de impacto social y económico.

## **TÍTULO IV – SOSTENIBILIDAD AMBIENTAL Y ENERGÉTICA**

**Artículo 8°** – La implementación de la presente ley deberá cumplir con las leyes ambientales y normas de sostenibilidad de la República Argentina, incluyendo la Ley General del Ambiente N° 25.675 y la Ley de Energías Renovables N° 27.191.

**Artículo 9°** – Los centros de datos, infraestructuras de inteligencia artificial y sistemas tecnológicos asociados a la RBT deberán incorporar fuentes de energía renovable, certificación de eficiencia energética y evaluación de impacto ambiental.

## **TÍTULO V – CONVERGENCIA INTERNACIONAL E INNOVACIÓN**

**Artículo 10°** – La presente ley se encuentra en consonancia con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de las Naciones Unidas, las recomendaciones del Banco Mundial, la OCDE y la OIT sobre fiscalidad en la economía digital, y las propuestas de redistribución tecnológica planteadas por Sam Altman, CEO de OpenAI.

**Artículo 11°** – Se reconoce la oportunidad que representa la llegada de empresas de inteligencia artificial al país, impulsando la cooperación público-privada para el desarrollo ético, inclusivo y soberano de la tecnología.

**Artículo 12° – Transparencia de la Propiedad Digital y Corporativa.**

El Estado promoverá la adopción progresiva del *Beneficial Ownership Data Standard (BODS)* desarrollado por *Open Ownership*, a fin de garantizar la trazabilidad, interoperabilidad y transparencia de la propiedad real de las empresas tecnológicas, nacionales y extranjeras que operen en territorio argentino.

Dicho proceso deberá coordinarse con los compromisos de la República Argentina ante la *Alianza para el Gobierno Abierto (OGP)* y las recomendaciones de la *OCDE* en materia de transparencia corporativa.

## TÍTULO VI – BENEFICIARIOS, ALCANCE Y GRADUALIDAD

**Artículo 12° – Beneficiarios de la Renta Básica Tecnológica**

Serán beneficiarios de la Renta Básica Tecnológica las personas humanas residentes en la República Argentina que cumplan con los criterios que establezca la reglamentación, priorizando:

- a) personas afectadas por procesos de automatización,
- b) trabajadores en transición laboral,
- c) sectores con alta vulnerabilidad tecnológica,
- d) jóvenes en formación digital,
- e) tareas de cuidado y economía social.

La RBT **no sustituye** políticas sociales existentes; las complementa.

---

**Artículo 13° – Universalidad progresiva**

La Renta Básica Tecnológica se implementará de manera **progresiva**, conforme:

- a) disponibilidad efectiva de financiamiento,
- b) impacto tecnológico medido,
- c) evaluaciones fiscales periódicas.

La universalidad será un **objetivo de mediano plazo**, no una obligación inmediata.

---

# TÍTULO VII – MONTO, MODALIDAD Y ACTUALIZACIÓN

## **Artículo 14° – Naturaleza del beneficio**

La Renta Básica Tecnológica tendrá carácter:

- personal,
  - intransferible,
  - no contributivo,
  - compatible con empleo y formación.
- 

## **Artículo 15° – Determinación del monto**

El monto de la RBT será fijado por la autoridad de aplicación en función de:

- a) ingresos efectivos del Fondo,
- b) indicadores de automatización sectorial,
- c) sostenibilidad fiscal,
- d) canasta digital mínima.

El monto **no podrá comprometer el equilibrio fiscal**.

---

## **Artículo 16° – Modalidad de pago**

La RBT se instrumentará preferentemente mediante:

- cuentas digitales públicas,
  - billeteras interoperables,
  - mecanismos trazables y auditables.
- 

# TÍTULO VIII – GOBERNANZA Y AUTORIDAD DE APLICACIÓN

## **Artículo 17° – Autoridad de aplicación**

Será autoridad de aplicación el organismo que designe el Poder Ejecutivo Nacional, con competencia en:

- 
- economía digital,
  - política social,
  - datos abiertos,
  - sostenibilidad tecnológica.
- 

### **Artículo 18° – Consejo Federal de Transición Digital**

Créase el Consejo Federal de Transición Digital, integrado por:

- Estado nacional,
- provincias,
- universidades,
- sector científico-tecnológico,
- sociedad civil especializada.

Su función será **asesora y evaluativa**, no ejecutiva.

---

## **TÍTULO IX – TRANSPARENCIA, CONTROL Y EVALUACIÓN**

### **Artículo 19° – Transparencia y datos abiertos**

Toda la información agregada del régimen deberá publicarse en formatos abiertos, garantizando:

- trazabilidad del financiamiento,
  - evaluación de impacto social,
  - auditoría ciudadana.
- 

### **Artículo 20° – Evaluación periódica**

La implementación de la RBT será evaluada cada **24 meses**, considerando:

- a) impacto social,
  - b) impacto laboral,
  - c) sostenibilidad fiscal,
  - d) impacto ambiental indirecto.
-

# **TÍTULO X – ARTICULACIÓN CON EL PAQUETE NORMATIVO**

## **Artículo 21° – Integración normativa obligatoria**

La presente ley se articula de manera directa con:

- Ley de Ampliación del RIGI,
- FONARETS,
- Ley de Transparencia y Beneficiarios Reales,
- Ley de Activos Estratégicos Externos,
- Ley de Datos Abiertos Soberanos.

Los recursos provenientes del RIGI Ampliado y FONARETS constituirán **fuente prioritaria** de financiamiento de la RBT.

---

# **TÍTULO XI – DISPOSICIONES FINALES**

## **Artículo 22° – Carácter no automático**

La RBT no constituye un derecho adquirido automático, sino un **instrumento de política pública sujeto a evaluación, financiamiento y sostenibilidad**.

---

## **Artículo 23° – Reglamentación**

El Poder Ejecutivo reglamentará la presente ley en un plazo máximo de **180 días**.

# FUNDAMENTOS

El avance acelerado de la inteligencia artificial (IA) y la automatización está transformando de manera estructural los mercados laborales, los sistemas de producción y las relaciones sociales. Este fenómeno, si bien ofrece oportunidades de progreso, también genera riesgos significativos de exclusión, desigualdad y pérdida de cohesión social.

La presente Ley de Renta Básica Tecnológica y Transición Digital Sostenible propone un nuevo contrato social basado en la redistribución equitativa del valor generado por el capital tecnológico, sustituyendo parcialmente la tributación tradicional sobre el trabajo por impuestos al capital digital y los beneficios extraordinarios de las empresas tecnológicas.

Inspirada en los principios del capitalismo inclusivo, la ley busca equilibrar crecimiento e inclusión: garantizar que los beneficios de la automatización sean compartidos por toda la sociedad. Este enfoque se alinea con los informes del Programa de las Naciones Unidas para el Desarrollo (PNUD) y la Organización Internacional del Trabajo (OIT), que instan a los Estados a crear mecanismos de protección social adaptados a la era digital.

Asimismo, el Banco Mundial y la OCDE recomiendan reformar los sistemas fiscales para gravar el capital digital y los rendimientos derivados de la automatización, permitiendo financiar políticas de reconversión laboral y renta básica universal. En el mismo sentido, la visión de Sam Altman, CEO de OpenAI, plantea la necesidad de redistribuir parte de los beneficios de la inteligencia artificial hacia los ciudadanos, mediante un sistema global o nacional de renta tecnológica.

Desde la perspectiva ambiental, la transición digital debe ser sostenible. La presente ley incorpora el cumplimiento de la Ley General del Ambiente N° 25.675 y la Ley de Energías Renovables N° 27.191, promoviendo el uso de fuentes limpias para las infraestructuras tecnológicas y la reducción de la huella ecológica de la inteligencia artificial.

Fiscalmente, la Renta Básica Tecnológica se concibe como un instrumento neutro o positivo: se financia mediante recursos efectivos derivados del capital, sin incrementar el gasto estructural del Estado. Este diseño asegura coherencia con los principios de equilibrio fiscal y superávit sostenible, fortaleciendo la estabilidad económica a largo plazo.

En síntesis, esta ley integra innovación, justicia social, sostenibilidad ambiental y

soberanía nacional en una misma propuesta. Su implementación permitirá que la Argentina lidere en América Latina una transición digital justa, inclusiva y fiscalmente responsable, basada en el principio de que el progreso tecnológico debe servir al bienestar humano y no sustituirlo.

**Firmado:**

**Natividad Vidal**

Autora del Proyecto

Capilla del Monte, Córdoba, Argentina

**Firma manuscrita digital:**



Natividad Vidal

DNI 27.716.481

**Correo institucional:**

datosabiertossoberanosar@gmail.com

**Acreditación:**

El presente proyecto es presentado en carácter de autora ciudadana y en cumplimiento de estándares internacionales de Gobierno Abierto, Transparencia Digital y Soberanía de Datos.

# **ANEXO I - INDICADORES DE AUTOMATIZACIÓN Y DESPLAZAMIENTO LABORAL**

## **Objetivo del anexo**

El presente anexo establece los **indicadores objetivos** para identificar sectores, actividades y regiones afectadas por procesos de automatización, digitalización intensiva o inteligencia artificial.

---

## **Indicadores principales**

Se considerarán, entre otros:

- a) porcentaje de tareas automatizables por sector,
  - b) incorporación de IA o robótica en procesos productivos,
  - c) reducción neta de empleo atribuible a tecnología,
  - d) sustitución de trabajo humano por sistemas algorítmicos,
  - e) concentración tecnológica en plataformas digitales.
- 

## **Fuentes de información**

Los indicadores se construirán a partir de datos de:

- organismos estadísticos nacionales,
  - universidades y centros de investigación,
  - informes sectoriales públicos,
  - datos abiertos del sistema productivo.
-

# **ANEXO II - METODOLOGÍA DE FINANCIAMIENTO DE LA RENTA BÁSICA TECNOLÓGICA**

## **Fuentes prioritarias**

La RBT se financiará prioritariamente con:

- a) aportes del FONARETS,
  - b) renta tecnológica extraordinaria,
  - c) cánones digitales y tecnológicos,
  - d) recupero de incentivos incumplidos del RIGI,
  - e) aportes internacionales para transición digital.
- 

## **Principio de sostenibilidad fiscal**

El financiamiento de la RBT deberá:

- ser verificable,
- no generar déficit estructural,
- ajustarse a la recaudación efectiva.

No se autoriza financiamiento vía endeudamiento permanente.

---

# **ANEXO III - CANASTA DIGITAL BÁSICA**

## **Definición**

Se entiende por **Canasta Digital Básica** el conjunto mínimo de bienes y servicios necesarios para la inclusión tecnológica efectiva.

---

## **Componentes mínimos**

La Canasta podrá incluir:

- a) conectividad básica,
  - b) acceso a dispositivos esenciales,
  - c) alfabetización digital,
  - d) servicios digitales públicos,
  - e) herramientas de formación y empleo digital.
- 

## **Actualización**

La Canasta será revisada periódicamente conforme evolución tecnológica y precios relativos.

---

# **ANEXO IV - ARTICULACIÓN CON EMPLEO, FORMACIÓN Y TRANSICIÓN LABORAL**

## **Complementariedad**

La RBT será compatible con:

- empleo formal,
- formación profesional,
- programas de reconversión laboral.

No desincentiva la inserción laboral.

---

## **Trayectorias de transición**

Se promoverán trayectorias que incluyan:

- a) formación técnica certificada,
- b) reconversión sectorial,

- c) inserción en economía del conocimiento,
  - d) apoyo a emprendimientos tecnológicos y sociales.
- 

## **ANEXO V - RÉGIMEN PILOTO, GRADUALIDAD Y EVALUACIÓN**

### **Implementación piloto**

La RBT se implementará inicialmente mediante **programas piloto**, priorizando:

- regiones de alto impacto tecnológico,
  - sectores críticos de transición,
  - colectivos vulnerables a automatización.
- 

### **Evaluación integral**

Los programas piloto serán evaluados considerando:

- a) impacto social,
  - b) impacto laboral,
  - c) impacto fiscal,
  - d) impacto territorial.
- 

### **Escalamiento responsable**

La ampliación del régimen estará condicionada a:

- resultados positivos verificables,
- sostenibilidad financiera,
- aprobación institucional.

# **PROYECTO DE LEY**

## **Ley de Sostenibilidad Tecnologica Ambiental de Argentina – 2025**

**Autora:**

Natividad Vidal

Capilla del Monte, Córdoba, Argentina

**Correo Institucional:** [datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

**Presentado ante:**

Honorable Cámara de Diputados de la Nación

Honorable Cámara de Senadores de la Nación

**Fecha:** \_\_\_\_\_

Proyecto presentado para su tratamiento en el marco del Programa de Soberanía Digital Argentina, alineado con estándares ONU – CEPAL – OGP.

## **PARTE I**

- INDICE GENERAL
- TÍTULO I — PRINCIPIOS GENERALES
- TÍTULO II — INFRAESTRUCTURA Y ENERGÍA
- TÍTULO III — CIRCULARIDAD Y FIN DE VIDA TECNOLÓGICO
- TÍTULO IV — INTELIGENCIA ARTIFICIAL Y AMBIENTE
- TÍTULO V — GOBERNANZA Y TRANSPARENCIA
- TÍTULO VI — MARCO SOBERANO DE CERTIFICACIÓN TECNOLÓGICA (MSCT)
- TÍTULO VII — TOKENIZACIÓN ÉTICA Y RESPONSABLE
- TÍTULO VIII — DISPOSICIONES FINALES
- TÍTULO IX — ECONOMÍA TOKENIZADA ÉTICA DE INTERCAMBIO COTIDIANO
- TÍTULO X - ENMARQUE INTERNACIONAL Y EJEMPLOS DE APLICACIÓN
- TÍTULO XI — ARTICULACIÓN CON EL MARCO AMBIENTAL NACIONAL
- FUNDAMENTOS

## **PARTE II**

- FIRMADOS

## **PARTE III**

- ANEXO I - DEFINICIONES TÉCNICAS NORMALIZADAS
- ANEXO II - METODOLOGÍA BASE DE EVALUACIÓN DE IMPACTO AMBIENTAL DIGITAL (EIAD)
- ANEXO III - ESQUEMA DE TRANSICIÓN PROGRESIVA HACIA LA SOSTENIBILIDAD TECNOLÓGICA
- ANEXO IV - GARANTÍAS DE NO MONETIZACIÓN Y NO FINANCIARIZACIÓN
- ANEXO V - EXPERIENCIAS PILOTO Y APLICACIÓN FEDERAL PROGRESIVA
- ANEXO VI - GLOSARIO CIUDADANO Y PRINCIPIOS DE COMUNICACIÓN PÚBLICA

- **ANEXO VII - ARTICULACIÓN CON LA LEY DE DATOS ABIERTOS SOBERANOS**
- **ANEXO VIII - ARTICULACIÓN CON LA LEY DE TOKENIZACIÓN ÉTICA**
- **ANEXO IX - INDICADORES DE SEGUIMIENTO Y CONTROL**
- **ANEXO X - CLÁUSULA DE EVOLUCIÓN TECNOLÓGICA**

# **PROYECTO DE LEY DE SOSTENIBILIDAD TECNOLÓGICA AMBIENTAL**

La presente ley forma parte del paquete legislativo por la Soberanía Digital Argentina. Su objetivo es garantizar que el desarrollo tecnológico nacional sea ambientalmente responsable, socialmente justo y soberano frente a los estándares extranjeros.

## **TÍTULO I — PRINCIPIOS GENERALES**

**Artículo 1°** — Objeto. La presente ley tiene por objeto garantizar el desarrollo, uso y desecho responsable de tecnologías digitales, promoviendo la sostenibilidad ambiental, energética y social del ecosistema tecnológico nacional.

**Artículo 2°** — Principios rectores. La política de sostenibilidad tecnológica se regirá por los principios de precaución ambiental, eficiencia energética, transparencia algorítmica, circularidad tecnológica, justicia intergeneracional y soberanía digital y ecológica.

**Artículo 3°** — Definición. Se entiende por sostenibilidad tecnológica la capacidad de desarrollar, utilizar y mantener tecnologías digitales minimizando sus impactos ecológicos y garantizando el respeto por los derechos humanos, laborales y ambientales.

## **TÍTULO II — INFRAESTRUCTURA Y ENERGÍA**

**Artículo 4°** — Centros de datos sostenibles. Todo centro de datos que opere en territorio nacional deberá utilizar energía proveniente de fuentes renovables, implementar sistemas de medición de consumo energético y publicar anualmente un Informe de Sostenibilidad Tecnológica.

**Artículo 5°** — Contrataciones públicas sostenibles. Toda licitación o compra pública tecnológica deberá incluir un Anexo de Impacto Ambiental y Energético (AIAE).

## **TÍTULO III — CIRCULARIDAD Y FIN DE VIDA TECNOLÓGICO**

**Artículo 6°** — Gestión de residuos electrónicos. El Estado deberá establecer un

Programa Nacional de Circularidad Tecnológica orientado a la reutilización y reciclado de equipos digitales en desuso.

**Artículo 7°** — Responsabilidad extendida del productor. Los fabricantes e importadores deberán garantizar la recolección y reciclado de al menos un 30% de los dispositivos comercializados anualmente.

## TÍTULO IV — INTELIGENCIA ARTIFICIAL Y AMBIENTE

### **Artículo 8° — Evaluación Ambiental de Sistemas Algorítmicos.**

Todo desarrollo o implementación pública de IA deberá incluir una Evaluación de Impacto Ambiental Digital (EIAD), obligatoria y pública, que analice consumo energético, huella de carbono e impacto del ciclo de vida tecnológico.

### **Artículo 9° — Principio de Sostenibilidad Tecnológica. Energía, agua y sostenibilidad obligatoria**

Los centros de datos, infraestructuras de inteligencia artificial, cómputo de alto rendimiento y sistemas tecnológicos asociados a la Red de Base Tecnológica (RBT) deberán cumplir obligatoriamente con los siguientes **estándares mínimos de sostenibilidad energética e hídrica**, sin perjuicio de las leyes ambientales vigentes.

#### **Artículo 9° bis – Abastecimiento energético renovable mínimo**

Todo centro de datos o infraestructura de IA deberá acreditar el siguiente **porcentaje mínimo de abastecimiento energético renovable**, calculado sobre su consumo anual total:

- a) **al menos 40 %** desde el inicio de operaciones,
- b) **al menos 60 %** a los tres (3) años,
- c) **al menos 80 %** a los cinco (5) años.

Las fuentes admitidas incluyen energía solar, eólica, biomasa, hidráulica de bajo impacto y otras renovables certificadas conforme la Ley N° 27.191.

#### **Artículo 9° ter – Autogeneración y compensación energética**

Al menos el **30 % del consumo energético renovable** deberá provenir de:

- a) autogeneración in situ o distribuida, o
- b) contratos de suministro renovable dedicados (PPA verdes).

El remanente podrá compensarse mediante certificados de energía renovable auditables, sin sustituir la obligación de eficiencia.

#### **Artículo 9º quater – Eficiencia energética obligatoria (PUE)**

Los centros de datos deberán cumplir con los siguientes **índices máximos de eficiencia energética (PUE – Power Usage Effectiveness)**:

- a) **PUE ≤ 1,6** en el primer año,
- b) **PUE ≤ 1,4** a los tres (3) años,
- c) **PUE ≤ 1,3** a los cinco (5) años.

La medición será anual, pública y auditada por la autoridad competente.

#### **Artículo 9º quinquies – Gestión y consumo de agua**

El uso de agua para refrigeración deberá cumplir con los siguientes criterios:

- a) **prioridad absoluta** a sistemas de refrigeración por aire, geotermia o circuito cerrado,
- b) **prohibición de uso de agua potable** cuando existan alternativas técnicas viables,
- c) reutilización mínima del **70 % del agua empleada**,
- d) utilización preferente de agua tratada, reciclada o de lluvia.

Se deberá presentar un **Plan de Gestión Hídrica** aprobado por la autoridad ambiental.

#### **Artículo 9º sexies – Indicador de eficiencia hídrica (WUE)**

Los centros de datos deberán reportar anualmente su **WUE (Water Usage Effectiveness)**, con los siguientes valores máximos orientativos:

- a) **WUE ≤ 1,8** en el primer año,
- b) **WUE ≤ 1,3** a los cinco (5) años.

La reglamentación podrá ajustar estos valores según región hídrica.

#### **Artículo 9º septies – Evaluación de Impacto Ambiental específica**

Toda infraestructura alcanzada deberá contar con:

- a) Evaluación de Impacto Ambiental específica para tecnologías digitales e IA,
- b) análisis de impacto energético, hídrico y térmico,
- c) evaluación de carga sobre redes eléctricas locales,
- d) planes de mitigación y compensación ambiental.

### **Artículo 9º octies – Transparencia y reporte público**

Los operadores deberán publicar anualmente, en formato abierto y agregable:

- a) consumo energético total,
- b) porcentaje de energía renovable utilizada,
- c) indicadores PUE y WUE,
- d) huella de carbono estimada,
- e) medidas de eficiencia implementadas.

### **Artículo 9º nonies – Régimen diferencial y gradualidad territorial**

La autoridad de aplicación podrá establecer **regímenes diferenciados** para:

- a) economías regionales,
- b) zonas con restricciones energéticas o hídricas,
- c) proyectos estratégicos de interés nacional,

sin reducir los estándares finales obligatorios, pero **permitiendo plazos razonables de adecuación**.

### **Artículo 9º decies – Condición para beneficios y habilitaciones**

El cumplimiento de los estándares establecidos en el presente artículo será **condición necesaria** para:

- a) acceder a beneficios fiscales o promocionales,
- b) recibir financiamiento público,
- c) obtener habilitaciones definitivas de operación.

## **TÍTULO V — GOBERNANZA Y TRANSPARENCIA**

**Artículo 10º** — Autoridad de aplicación. Créase la Agencia Nacional de Sostenibilidad Tecnológica (ANST), bajo la órbita del Ministerio de Ambiente y en coordinación con la Secretaría de Innovación Pública.

**Artículo 11º** — Consejo Asesor Multisectorial. Se conformará un consejo con universidades, sociedad civil, sector privado y organismos internacionales para elaborar estándares nacionales de sostenibilidad digital.

**Artículo 11 bis** — Elaboración de Estándares Nacionales de Sostenibilidad Digital. La ANST elaborará y actualizará cada tres años los ENSD, que incluirán normas de

eficiencia energética, evaluación ambiental digital, transparencia algorítmica, circularidad tecnológica, ética social e indicadores de cumplimiento.

## TÍTULO VI — MARCO SOBERANO DE CERTIFICACIÓN TECNOLÓGICA (MSCT)

**Artículo 16°** — Creación. Créase el Marco Soberano de Certificación Tecnológica (MSCT) para verificar el cumplimiento de los ENSD sin depender de normas extranjeras.

**Artículo 17°** — Autoridad de aplicación. El MSCT será administrado por la ANST en coordinación con el INTI y la Secretaría de Innovación Pública, con participación de universidades nacionales y cooperativas tecnológicas.

**Artículo 18°** — Objetivos. El MSCT evaluará infraestructura, eficiencia energética, circularidad y justicia digital, evitando la dependencia de certificaciones foráneas.

**Artículo 19°** — Categorías de certificación. Se establecen tres niveles: Nivel I – Cumplimiento básico; Nivel II – Sostenibilidad integral; Nivel III – Innovación soberana. Se otorgará el Sello Soberano Digital-AR.

**Artículo 20°** — Auditorías y transparencia. La ANST publicará anualmente el listado de entidades certificadas y sus informes de evaluación.

**Artículo 21°** — Cooperación regional. Argentina podrá suscribir acuerdos de reconocimiento recíproco con países latinoamericanos para crear el Bloque Regional de Certificación Tecnológica del Sur (CERTEC-SUR).

**Artículo 22°** — Incentivos. Las entidades que obtengan el Sello Soberano Digital-AR accederán a beneficios fiscales y prioridad en contrataciones públicas tecnológicas.

## TÍTULO VII — TOKENIZACIÓN ÉTICA Y RESPONSABLE

**Artículo 23°** — Tokenización Ética y Responsable. Se reconoce la tokenización ética como instrumento legítimo de certificación, trazabilidad y participación digital, siempre que cumpla con los principios de transparencia, consentimiento informado, equidad, sostenibilidad energética y prohibición de especulación de datos personales.

**Artículo 24°** — Sistema Nacional de Tokenización Ética (SINTE). Créase el SINTE, administrado por la ANST, para certificar proyectos blockchain o de tokenización con finalidad ambiental, científica o social. Los proyectos aprobados recibirán el Sello

'Token Ético Argentino (TEA)'.

**Artículo 25°** — Principios operativos. Toda tokenización deberá priorizar redes de bajo consumo, infraestructura soberana y reinversión nacional del valor generado. Se prohíbe la tokenización de datos personales o biométricos sin consentimiento ciudadano.

**Artículo 26°** — Coordinación interinstitucional. El SINTE actuará en coordinación con el Banco Central, la Comisión Nacional de Valores y el Ministerio de Ambiente para establecer lineamientos comunes de trazabilidad y finanzas sostenibles digitales.

## TÍTULO VIII — DISPOSICIONES FINALES

**Artículo 27°** — Reglamentación. El Poder Ejecutivo reglamentará la presente ley en un plazo de 180 días desde su promulgación.

**Artículo 28°** — Adhesión provincial. Invítase a las provincias y municipios a adherir a la presente ley, creando sus propios planes de sostenibilidad tecnológica.

**Artículo 29°** — Vigencia. La presente ley entrará en vigencia a los 30 días de su publicación en el Boletín Oficial.

## TÍTULO IX — ECONOMÍA TOKENIZADA ÉTICA DE INTERCAMBIO COTIDIANO

### Articulo 30° - Propósito general

Promover un sistema de **tokenización ética soberana** destinado a incentivar prácticas sostenibles, saludables y socialmente valiosas en la vida cotidiana de la población. El objetivo es integrar los avances tecnológicos con políticas públicas que refuerzen el bienestar, la eficiencia energética y la inclusión digital, sin sustituir la moneda nacional ni generar dependencia de redes privadas o especulativas.

### Articulo 31° - Principios orientadores

- **Soberanía digital:** los tokens se emiten, gestionan y auditán bajo infraestructura nacional.
- **Transparencia y voluntariedad:** toda participación ciudadana es libre, informada y anónima.

- **No especulación:** los tokens no cotizan ni se compran; representan valor social, ambiental o cultural.
- **Reinversión nacional:** cada token canjeado se traduce en beneficio directo al territorio (educación, energía, salud o cultura).
- **Sostenibilidad ambiental:** el sistema prioriza redes blockchain o bases de datos energéticamente eficientes y abiertas.

## Articulo 32° - Tipología de tokens soberanos propuestos

Nombre del token	Finalidad principal	Ejemplo de uso
<b>Token Verde Argentino (TVA)</b>	Premiar ahorro energético, reciclaje o transporte limpio.	Descuentos en transporte público, bonos de eficiencia, programas de energía solar.
<b>Token Saludable Argentino (TSA)</b>	Fomentar actividad física y alimentación sana.	Descuentos en gimnasios, mercados saludables o cheques médicos.
<b>Token Cultural Argentino (TCA)</b>	Promover participación artística, comunitaria o educativa.	Entradas gratuitas a museos, festivales o cursos públicos.
<b>Token Laboral Soberano (TLS)</b>	Reconocer empleos verdes, cooperativos o tecnológicos.	Bonificaciones en servicios, formación o aportes previsionales.
<b>Token Ciudadano Ético (TCE)</b>	Recompensar participación en consultas públicas o presupuestos participativos.	Créditos para capacitaciones o beneficios sociales.

## Articulo 33° - Estructura operativa

- **Autoridad coordinadora:** Agencia Nacional de Sostenibilidad Tecnológica (ANST), junto al Banco Central y la Secretaría de Innovación Pública.
- **Plataforma soberana:** “**MiToken.AR**”, una billetera digital ciudadana interoperable con servicios públicos y privados adheridos.

- **Gestión de emisión:** cada token tiene un respaldo en acción o impacto verificado (por ejemplo, kilovatios ahorrados, actividad física registrada o eventos culturales participados).
- **Destrucción programada:** los tokens se eliminan al canjearse, evitando acumulación o especulación.

## **Articulo 34° - Casos de uso aplicables**

### **Alimentación**

- Obtención de **Token Saludable** al comprar productos locales o agroecológicos.
- Canje en ferias municipales o mercados regionales.

### **Transporte**

- **Token Verde** por uso de transporte público, bicicleta o autos compartidos.
- Canje directo por saldo SUBE o pasajes de tren interurbano.

### **Educación y cultura**

- **Token Cultural** otorgado por asistencia a cursos, talleres o actividades artísticas.
- Canje por libros digitales o acceso a plataformas educativas nacionales.

### **Trabajo y economía social**

- **Token Laboral** emitido por cooperativas o pymes certificadas sostenibles.
- Usable como crédito fiscal o acceso a beneficios previsionales.

## **Articulo 35° - Garantías éticas**

- Anonimato criptográfico sin perfilado personal.
- Acceso universal e inclusivo (funcionamiento sin smartphone mediante DNI o tarjeta ciudadana).
- Auditoría pública permanente del código, las métricas y los flujos de valor.
- Publicación de todos los indicadores en el **Portal Nacional de Datos Abiertos**.

## **Aritulo 36° - Vinculación con la Ley de Sostenibilidad Tecnológica**

El sistema de tokenización cotidiana forma parte del **Marco Soberano de Certificación Tecnológica (MSCT)** y se coordina con el **Sistema Nacional de Tokenización Ética (SINTE)**, garantizando coherencia entre sostenibilidad ambiental, innovación digital y justicia social.

La reglamentación podrá establecer convenios con provincias, municipios, universidades y cooperativas para desarrollar **pilotos locales de economía tokenizada ética**, asegurando una transición gradual y soberana hacia nuevas formas de intercambio responsable.

## **TITULO X - ENMARQUE INTERNACIONAL Y EJEMPLOS DE APLICACIÓN**

### **Articulo 37° - Enmarca global**

El desarrollo del sistema de **tokenización ética soberana** se articula con los siguientes instrumentos internacionales:

#### **Agenda 2030 de Naciones Unidas**

- **ODS 7:** Energía asequible y no contaminante.
- **ODS 9:** Industria, innovación e infraestructura.
- **ODS 12:** Producción y consumo responsables.
- **ODS 13:** Acción por el clima.
- **ODS 16-17:** Instituciones sólidas y alianzas para el desarrollo.

#### **ONU — Roadmap for Digital Cooperation (2021)**

- *Principio 2:* Asegurar que la transformación digital beneficie a las personas y al planeta.
- *Principio 5:* Reforzar la confianza digital mediante gobernanza de datos y transparencia.

#### **Carta de Principios de Gobernanza Digital Abierta (OGP 2022)**

Compromisos III, V y VI sobre transparencia tecnológica, inclusión y co-creación digital.

#### **Declaración OCDE sobre Transición Digital Justa y Verde (2023)**

Puntos 8 y 9: promover tecnologías verdes e independencia tecnológica.

## Artículo 38° - Ejemplos internacionales de referencia

Iniciativa	Región	Rasgo principal	Adaptación argentina sugerida
<b>Chia Network / Toucan Protocol</b>	EE.UU./UE/LatAm	Tokenización de créditos de carbono.	<i>Token Verde Argentino (TVA)</i> para trazabilidad de emisiones.
<b>Iniciativa Región Rasgo principal Adaptación argentina sugerida</b>			
<b>Circularise</b>	Unión Europea	Blockchain para seguimiento de materiales reciclados.	<i>Token Circular AR (TCAR)</i> para residuos tecnológicos.
<b>Estonia Digital ID Tokens</b>	Estonia	Identidad digital tokenizada.	<i>Token Identitario Soberano (TIS)</i> sin datos biométricos.
<b>Knowledge NFTs (UNESCO Labs)</b>	Multilateral	Tokenización ética del conocimiento científico.	<i>Token Soberano del Conocimiento (TSK)</i> en universidades públicas.
<b>SDG Impact Tokens (PNUD)</b>	Global	Tokens de trazabilidad de impacto social.	<i>Token Ciudadano Ético (TCE)</i> para medir acción climática y participación.

## Artículo 39° - Adaptación al contexto argentino

1. **Descentralización soberana:** infraestructura alojada en centros de datos nacionales certificados.
2. **Inclusión social:** integración con SUBE, Mercado Federal, PAMI Digital, pensionados discapacidad y universidades.
3. **Economía circular digital:** incentivos ligados a eficiencia energética, salud y cooperativismo.

## **Articulo 40° - Vinculación institucional**

El sistema contribuye a los compromisos internacionales de la Argentina en:

- Transición digital justa (ONU-OCDE 2023).
- Carta Iberoamericana de Derechos Digitales (SEGIB 2022).
- Iniciativa Latinoamericana de IA Ética (CEPAL – UNESCO – BID).

**Referencia:** *Lineamientos Globales de Transición Digital Justa*, Artículo 4 –

“Los Estados deberán asegurar que la digitalización contribuya al desarrollo sostenible, respetando la soberanía de datos, la equidad social y la protección ambiental.”

# **TÍTULO XI — ARTICULACIÓN CON EL MARCO AMBIENTAL NACIONAL**

## **Articulo 41° - Vinculación normativa**

La presente ley se integra al marco jurídico ambiental argentino, complementando y respetando los principios establecidos en:

- **Ley General del Ambiente N.º 25.675 (2002):** Política ambiental nacional y principios de prevención, equidad intergeneracional y sustentabilidad.
- **Ley de Bosques Nativos N.º 26.331 (2007):** Ordenamiento territorial de los bosques nativos.
- **Ley de Glaciares N.º 26.639 (2010):** Preservación de glaciares y ambiente periglacial.
- **Ley de Presupuestos Mínimos de Cambio Climático N.º 27.520 (2019):** Planes nacionales de mitigación y adaptación.
- **Ley de Protección de los Recursos Hídricos N.º 25.688 (2002):** Gestión integrada y uso racional del agua.
- **Ley de Residuos Peligrosos N.º 24.051 (1992):** Manejo responsable de residuos.

- **Ley de Tierras Rurales N.º 26.737 (2011):** Protección de la propiedad nacional y soberanía territorial.

#### **Articulo 42° - Complementariedad funcional**

La Ley de Sostenibilidad Tecnológica actúa como marco transversal que:

- Integra la dimensión digital dentro de la política ambiental.
- Obliga a que toda infraestructura tecnológica cumpla evaluaciones ambientales según la Ley 25.675.
- Refuerza la soberanía sobre territorio, datos e infraestructura digital conforme a la Ley 26.737.
- Vincula los proyectos tecnológicos con los planes climáticos de la Ley 27.520.
- Garantiza que toda política tecnológica respete los principios de precaución, equidad y sustentabilidad.

#### **Articulo 43° - Enfoque de sostenibilidad integral**

Su aplicación debe asegurar que:

1. Las políticas de innovación y digitalización evalúen impacto ambiental y social.
2. Las inversiones tecnológicas (centros de datos, IA, redes, minería digital) se ajusten al marco ambiental nacional.
3. La innovación tecnológica contribuya también a la restauración ecológica y la regeneración de ecosistemas.

#### **Articulo 44° - Coordinación interinstitucional**

Se promoverá un **Convenio de Integración Ambiental-Tecnológica** entre:

- Ministerio de Ambiente y Desarrollo Sostenible,
- Secretaría de Innovación Pública,
- Ministerio de Ciencia, Tecnología e Innovación,
- Consejo Federal de Medio Ambiente (COFEMA).

El convenio establecerá protocolos conjuntos de evaluación, certificación y monitoreo de proyectos digitales con impacto ambiental.

#### **Artículo 45º - Principio de coherencia normativa**

Toda reglamentación derivada de esta ley deberá interpretarse conforme al **artículo 41 de la Constitución Nacional**, que garantiza el derecho a un ambiente sano y sostenible.

El desarrollo tecnológico argentino deberá respetar los **límites ecológicos del territorio** y promover una **transición digital ambientalmente justa, equitativa y soberana**.

## **FUNDAMENTOS**

El presente proyecto de Ley de Sostenibilidad Tecnológica busca alinear la transición digital argentina con los Objetivos de Desarrollo Sostenible (ODS 7, 12 y 13), el Acuerdo de París y la Agenda Digital 2030. La incorporación del Título VII sobre Tokenización Ética garantiza que los mecanismos de trazabilidad y valor digital respeten principios éticos, ambientales y soberanos, fortaleciendo la independencia tecnológica del país.

**Firmado:**

**Natividad Vidal**

Autora del Proyecto

Capilla del Monte, Córdoba, Argentina

**Firma manuscrita digital:**



Natividad Vidal

DNI 27.716.481

**Correo institucional:**

[datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

**Acreditación:**

El presente proyecto es presentado en carácter de autora ciudadana y en cumplimiento de estándares internacionales de Gobierno Abierto, Transparencia Digital y Soberanía de Datos.

# **ANEXO I - DEFINICIONES TÉCNICAS NORMALIZADAS**

A los efectos de la presente ley y de su reglamentación, se adoptan las siguientes definiciones:

## **1. Sostenibilidad tecnológica**

Capacidad de diseñar, desarrollar, implementar, mantener y desechar tecnologías digitales minimizando impactos ambientales, energéticos y sociales, garantizando derechos humanos, laborales, ambientales y soberanía tecnológica.

## **2. Infraestructura tecnológica soberana**

Conjunto de sistemas, centros de datos, redes, plataformas y servicios digitales:

- a. alojados en territorio nacional o bajo jurisdicción argentina,
- b. regidos por normativa nacional,
- c. auditables por organismos públicos,
- d. no subordinados a estándares o certificaciones extranjeras obligatorias.

## **3. Red de bajo consumo energético**

Infraestructura digital cuya operación prioriza eficiencia energética, uso de energías renovables y mecanismos de reducción de huella de carbono, incluyendo redes blockchain de prueba de participación u otros sistemas equivalentes de bajo impacto ambiental.

## **4. Circularidad tecnológica**

Modelo de gestión que extiende el ciclo de vida de dispositivos digitales mediante reutilización, reparación, reciclado y rediseño, evitando la obsolescencia

programada y la generación innecesaria de residuos electrónicos.

## **5. Token no especulativo**

Unidad digital de registro que representa valor social, ambiental, cultural o funcional, sin cotización en mercados financieros, sin posibilidad de compraventa, acumulación especulativa ni generación de renta privada.

## **6. Anonimato criptográfico**

Protección técnica de la identidad ciudadana mediante mecanismos criptográficos que permiten verificar acciones o impactos sin revelar datos personales ni generar perfiles individualizados.

# **ANEXO II - METODOLOGÍA BASE DE EVALUACIÓN DE IMPACTO AMBIENTAL DIGITAL (EIAD)**

La Evaluación de Impacto Ambiental Digital (EIAD) deberá contemplar, como mínimo, los siguientes ejes:

## **1. Consumo energético**

- Energía directa utilizada por la infraestructura.
- Energía indirecta asociada a almacenamiento, transmisión y procesamiento de datos.

## **2. Huella de carbono**

- Emisiones derivadas del ciclo de vida tecnológico.
- Compensaciones o mitigaciones previstas.

## **3. Uso de recursos naturales**

- Consumo de agua.
- Uso de materiales críticos o escasos.

## **4. Ciclo de vida tecnológico**

- Durabilidad del hardware.
- Posibilidades de reutilización o reciclado.
- Gestión de residuos electrónicos.

## **5. Impacto territorial y social**

- Localización de la infraestructura.
- Impacto en comunidades locales.

- Condiciones laborales asociadas.

La EIAD deberá ser **pública, accesible y reutilizable**, conforme a la Ley de Datos Abiertos.

## **ANEXO III - ESQUEMA DE TRANSICIÓN PROGRESIVA HACIA LA SOSTENIBILIDAD TECNOLÓGICA**

Con el fin de garantizar viabilidad técnica y equidad territorial, se establece un esquema de transición progresiva:

### **1. Centros de datos e infraestructura crítica**

- Año 1: mínimo 40 % de energía renovable.
- Año 3: mínimo 70 % de energía renovable.
- Año 5: objetivo del 100 %, salvo excepciones debidamente justificadas.

### **2. Certificación MSCT**

- Adhesión voluntaria inicial.
- Obligatoriedad progresiva para contrataciones públicas.

### **3. Evaluaciones ambientales digitales**

- Aplicación prioritaria en proyectos nuevos.
- Adecuación gradual de sistemas existentes.

La reglamentación podrá contemplar particularidades regionales y excepciones transitorias fundadas.

## **ANEXO IV - GARANTÍAS DE NO MONETIZACIÓN Y NO FINANCIARIZACIÓN**

1. Los sistemas de tokenización previstos en la presente ley:

- no constituyen moneda,
- no reemplazan ni compiten con la moneda de curso legal,
- no generan deuda pública ni privada,
- no habilitan instrumentos financieros.

2. Los tokens:

- no cotizan en mercados,
- no pueden ser comprados ni vendidos,
- se extinguen al momento de su canje.

3. Queda expresamente prohibida:

- la intermediación financiera privada,
- la especulación,
- la acumulación patrimonial derivada de tokens soberanos.

4. Toda operatoria deberá respetar los principios de:

- transparencia,
- consentimiento informado,
- anonimato,
- soberanía de datos.

## **ANEXO V - EXPERIENCIAS PILOTO Y APLICACIÓN FEDERAL**

# **PROGRESIVA**

## **1. Objeto del anexo**

Establecer lineamientos para la implementación de experiencias piloto de sostenibilidad tecnológica y tokenización ética en jurisdicciones subnacionales, universidades públicas, cooperativas y organismos descentralizados.

## **2. Ámbitos habilitados**

Podrán desarrollarse experiencias piloto en:

- Municipios y comunas.
- Provincias adherentes.
- Universidades nacionales.
- Cooperativas tecnológicas y energéticas.
- Programas sociales, educativos, culturales o ambientales.

## **3. Criterios de selección**

Las experiencias piloto deberán:

- responder a necesidades locales verificables,
- utilizar infraestructura soberana,
- respetar anonimato y no monetización,
- publicar resultados en el Portal Nacional de Datos Abiertos.

## **4. Duración y evaluación**

- Plazo sugerido: 12 a 24 meses.
- Evaluación pública de impacto ambiental, social y tecnológico.
- Posibilidad de escalamiento nacional mediante reglamentación.

## **5. Federalismo tecnológico**

Este anexo garantiza que la transición digital sostenible:

- no sea centralista,
- respete autonomías provinciales,
- promueva capacidades locales.

# **ANEXO VI - GLOSARIO CIUDADANO Y PRINCIPIOS DE COMUNICACIÓN PÚBLICA**

## **1. Finalidad**

Asegurar que la aplicación de la ley sea comprendida por la ciudadanía, promoviendo transparencia, alfabetización digital y participación informada.

## **2. Lineamientos de comunicación**

Toda comunicación pública asociada a la ley deberá:

- utilizar lenguaje claro,
- evitar tecnicismos innecesarios,
- explicar derechos y garantías,
- informar sobre mecanismos de control ciudadano.

## **3. Conceptos clave en lenguaje ciudadano**

Ejemplos orientativos:

- *Sostenibilidad tecnológica*: usar tecnología sin dañar el ambiente ni a las personas.
- *Token ético*: reconocimiento digital por acciones positivas, no dinero.
- *Infraestructura soberana*: sistemas tecnológicos que responden a leyes argentinas.
- *Datos abiertos*: información pública accesible para todos.

## **4. Participación ciudadana**

Se promoverán:

- consultas públicas,
- instancias educativas,
- materiales abiertos reutilizables.

# **ANEXO VII - ARTICULACIÓN CON LA LEY DE DATOS ABIERTOS SOBERANOS**

## **1. Principio de coherencia normativa**

Toda información generada por la aplicación de la Ley de Sostenibilidad Tecnológica deberá regirse por los principios de:

- apertura por defecto,
- trazabilidad,
- reutilización,
- protección de datos personales.

## **2. Datos obligatoriamente abiertos**

Deberán publicarse:

- informes EIAD,
- certificaciones MSCT,
- auditorías del SINTE,
- métricas de tokenización ética.

## **3. Excepciones**

Solo podrán exceptuarse:

- datos sensibles protegidos por ley,
- información que comprometa seguridad crítica,
- datos personales no anonimizables.

# **ANEXO VIII - ARTICULACIÓN CON LA LEY DE TOKENIZACIÓN ÉTICA**

## **1. Marco de complementariedad**

La tokenización prevista en la presente ley se integra al régimen general de Tokenización Ética, actuando como:

- aplicación ambiental,
- instrumento de trazabilidad,
- mecanismo de incentivo no monetario.

## **2. Prelación normativa**

En caso de conflicto interpretativo:

- prevalecerán los principios de no especulación,
- sostenibilidad ambiental,
- soberanía tecnológica.

## **3. Unificación de registros**

El SINTE actuará como registro único nacional, evitando superposición de sistemas.

# **ANEXO IX - INDICADORES DE SEGUIMIENTO Y CONTROL**

## **1. Indicadores mínimos**

- consumo energético del ecosistema digital público,
- porcentaje de energía renovable,
- volumen de residuos electrónicos recuperados,
- cantidad de proyectos certificados MSCT,
- cantidad de tokens emitidos y extinguidos.

## **2. Publicación**

Los indicadores deberán:

- actualizarse periódicamente,
- publicarse en formato abierto,
- permitir auditoría ciudadana.

# **ANEXO X - CLÁUSULA DE EVOLUCIÓN TECNOLÓGICA**

## **1. Principio de adaptabilidad**

La aplicación de la ley deberá interpretarse de forma dinámica, permitiendo incorporar:

- nuevas tecnologías,
- mejoras en eficiencia energética,
- estándares soberanos emergentes.

## **2. Límite infranqueable**

Ninguna actualización podrá vulnerar:

- derechos humanos,
- principios ambientales,
- soberanía de datos,
- prohibición de especulación.

# **ANEXO X - SOSTENIBILIDAD EN CENTROS DE DATOS, INTELIGENCIA ARTIFICIAL Y CÓMPUTO DE ALTA DEMANDA**

## **Ámbito de aplicación**

El presente anexo será de **aplicación obligatoria** para:

- a) centros de datos de mediana y gran escala,
- b) infraestructuras de inteligencia artificial, machine learning y HPC,
- c) nubes públicas, privadas o híbridas,

- d) infraestructuras tecnológicas asociadas a la Red de Base Tecnológica (RBT),
- e) proyectos nuevos y ampliaciones significativas de proyectos existentes.

### **Clasificación por escala de consumo**

A los fines regulatorios, los centros de datos se clasifican según su consumo eléctrico anual:

- a) **Categoría I (media)**: hasta 10 MW
- b) **Categoría II (alta)**: entre 10 MW y 50 MW
- c) **Categoría III (crítica)**: más de 50 MW

Las exigencias se aplicarán con mayor rigor a partir de la Categoría II.

### **Abastecimiento energético renovable obligatorio**

Los centros alcanzados deberán cumplir con los siguientes **mínimos obligatorios**:

#### **Año de operación % mínimo renovable**

Inicio	40 %
Año 3	60 %
Año 5	80 %

Para Categoría III, el porcentaje mínimo a los cinco años será **90 %**.

### **Autogeneración y contratos verdes**

Al menos el **30 % del consumo renovable** deberá provenir de:

- a) autogeneración in situ o distribuida,
- b) contratos PPA renovables dedicados,
- c) parques energéticos asociados.

Los certificados de compensación no podrán superar el **50 % del total renovable declarado**.

### **Eficiencia energética obligatoria (PUE)**

Los centros deberán cumplir con los siguientes valores máximos de **PUE**:

#### **Etapa PUE máximo**

### **Etapa PUE máximo**

Inicio 1,6

Año 3 1,4

Año 5 1,3

Para proyectos nuevos de Categoría III: **PUE inicial ≤ 1,4.**

### **Gestión térmica y diseño eficiente**

Será obligatorio:

- a) diseño pasivo y orientación eficiente,
- b) recuperación de calor residual cuando sea técnicamente viable,
- c) priorización de refrigeración por aire, free cooling o geotermia,
- d) prohibición de tecnologías obsoletas de alto consumo.

### **Uso y protección del recurso hídrico**

El uso de agua deberá cumplir:

- a) prohibición de uso de agua potable cuando existan alternativas,
- b) reutilización mínima del **70 %**,
- c) uso preferente de agua tratada, reciclada o pluvial,
- d) circuitos cerrados de refrigeración.

Toda instalación deberá contar con **Plan de Gestión Hídrica aprobado**.

### **Indicador de eficiencia hídrica (WUE)**

Valores máximos orientativos:

### **Etapa WUE máximo**

Inicio 1,8

Año 5 1,3

La autoridad de aplicación podrá ajustar valores según estrés hídrico regional.

### **Evaluación de impacto ambiental digital**

La Evaluación de Impacto Ambiental deberá incluir:

- a) carga sobre redes eléctricas locales,
- b) impacto hídrico y térmico,
- c) huella de carbono directa e indirecta,
- d) planes de mitigación y compensación,
- e) análisis de resiliencia energética.

### **Transparencia y reporte obligatorio**

Los operadores deberán publicar anualmente:

- a) consumo energético total,
- b) porcentaje renovable real,
- c) PUE y WUE,
- d) emisiones asociadas,
- e) planes de mejora.

La información será pública, agregada y auditada.

### **Restricciones territoriales y protección local**

No se autorizarán centros de datos de Categoría II o III en:

- a) zonas con estrés hídrico crítico,
- b) regiones con déficit energético estructural,
- c) áreas protegidas o sensibles,

salvo que el proyecto **demuestre autoabastecimiento energético e hídrico**.

### **Condición para habilitación y beneficios**

El cumplimiento del presente anexo será condición necesaria para:

- a) habilitación definitiva,
- b) acceso a beneficios fiscales,
- c) inclusión en regímenes promocionales,
- d) contratación con el Estado.

---

### **Actualización tecnológica**

Los estándares del presente anexo podrán actualizarse cada cinco (5) años, manteniendo siempre el principio de **no regresividad ambiental y tecnológica**.

# **PROYECTO DE LEY**

## **Ley de Ciberseguridad, Identidad Digital y Transformacion Digital de Argentina – 2025**

### **Autora:**

Natividad Vidal

Capilla del Monte, Córdoba, Argentina

**Correo Institucional:** [datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

### **Presentado ante:**

Honorable Cámara de Diputados de la Nación

Honorable Cámara de Senadores de la Nación

**Fecha:** \_\_\_\_\_ (colocar al momento de presentación)



Natividad Vidal

DNI 27.716.481

Proyecto presentado para su tratamiento en el marco del Programa de Soberanía Digital Argentina, alineado con estándares ONU – CEPAL – OGP.

## **PARTE I**

- **ÍNDICE GENERAL**
- **TÍTULO I — DISPOSICIONES GENERALES**
- **TÍTULO II — PROTECCIÓN DE LOS DATOS PERSONALES Y GESTIÓN ÉTICA DE LOS DATOS**
- **TÍTULO III — INTELIGENCIA ARTIFICIAL EN POLÍTICAS PÚBLICAS**
- **TÍTULO IV — IDENTIDAD DIGITAL Y DOCUMENTOS ELECTRÓNICOS**
- **TÍTULO V — TELECOMUNICACIONES, ACCESO Y COMPETITIVIDAD TECNOLÓGICA**
- **TÍTULO VI — ECONOMÍA DIGITAL, COMERCIO Y CONSUMIDORES**
- **TÍTULO VII — TRABAJO, EDUCACIÓN Y SALUD DIGITALES**
- **TÍTULO VIII — COMPRAS PÚBLICAS E INNOVACIÓN**
- **TÍTULO IX — AUTORIDAD DE APLICACIÓN Y COORDINACIÓN**
- **TÍTULO X — DISPOSICIONES FINALES**
- **TÍTULO XI — MARCO NACIONAL DE INTELIGENCIA ARTIFICIAL Y TRANSPARENCIA ALGORÍTMICA**
- **TÍTULO XII — TELECOMUNICACIONES, CONECTIVIDAD Y DESARROLLO TECNOLÓGICO COMPETITIVO**
- **TÍTULO XIII — ECONOMÍA DIGITAL, COMERCIO ELECTRÓNICO Y PROTECCIÓN DEL CONSUMIDOR**
- **TÍTULO XIV — DERECHOS LABORALES DIGITALES Y TELETRABAJO ÉTICO**
- **TÍTULO XV — GOBERNANZA DIGITAL Y COORDINACIÓN INTERINSTITUCIONAL**

## **PARTE II**

- **FIRMADOS**

## **PARTE III**

- **ANEXO I - INFRAESTRUCTURA CRÍTICA DIGITAL (ICD)**
- **ANEXO II - NIVELES DE RIESGO CIBERNÉTICO Y CLASIFICACIÓN**
- **ANEXO III - PROTOCOLOS DE INCIDENTES, RESPUESTA Y REVERSIÓN**
- **ANEXO IV - CERTIFICACIONES, ESTÁNDARES Y AUDITORÍAS**
- **ANEXO V - COORDINACIÓN FEDERAL, COOPERACIÓN Y TRANSICIÓN**

# **PROYECTO DE LEY DE CIBERSEGURIDAD, IDENTIDAD DIGITAL Y TRANSFORMACIÓN DIGITAL DE ARGENTINA**

## **TÍTULO I — DISPOSICIONES GENERALES**

### **Artículo 1° — Objeto**

La presente ley tiene por objeto establecer un marco normativo integral que:

- a) Garantice la seguridad y confianza en el entorno digital.
- b) Proteja la identidad digital y los datos personales.
- c) Promueva la innovación, la inclusión digital y la competitividad tecnológica.
- d) Asegure un ciberespacio abierto, seguro y respetuoso de los derechos humanos.
- e) Fortalezca la soberanía tecnológica nacional y la cooperación internacional responsable.

### **Artículo 2° — Principios**

- 1. Seguridad con derechos.
- 2. Responsabilidad compartida.
- 3. Prevención, reparación y reversibilidad.
- 4. Transparencia y ética en el tratamiento de datos.
- 5. Interoperabilidad y cooperación.
- 6. Principio de “solicitar solo una vez”.
- 7. Innovación responsable.

## **TÍTULO II — PROTECCIÓN DE LOS DATOS PERSONALES Y GESTIÓN ÉTICA DE LOS DATOS**

### **Capítulo I — Principios y Alcance**

#### **Artículo 3° — Objeto.**

El presente Título tiene por objeto garantizar la protección integral de los datos personales y sensibles, promover la gestión ética y responsable de la información y establecer los mecanismos para el tratamiento, intercambio e interoperabilidad de datos en el sector público y privado.

#### **Artículo 4º — Principios rectores.**

Toda actividad de recolección, tratamiento, intercambio o almacenamiento de datos deberá regirse por los siguientes principios:

- a) Licitud y finalidad: el tratamiento debe fundarse en base legal expresa y responder a un propósito legítimo y determinado.
- b) Transparencia y trazabilidad: los ciudadanos deberán poder conocer en todo momento quién, cómo y para qué se usan sus datos.
- c) Minimización: sólo podrán recopilarse los datos estrictamente necesarios para el cumplimiento de la finalidad declarada.
- d) Integridad y seguridad: deberán implementarse medidas técnicas y organizativas adecuadas para prevenir accesos, pérdidas o alteraciones no autorizadas.
- e) Responsabilidad proactiva: los responsables del tratamiento deberán demostrar el cumplimiento de las obligaciones establecidas por esta ley.
- f) Principio de solicitar solo una vez: ninguna entidad pública podrá requerir a los ciudadanos información que ya obre en poder del Estado.

### **Capítulo II — Tratamiento e Intercambio de Datos**

#### **Artículo 5º — Tratamiento en el sector público.**

Los organismos públicos deberán establecer políticas de tratamiento de datos personales bajo estándares de interoperabilidad, seguridad y control ciudadano, asegurando que la información recopilada se utilice únicamente para los fines administrativos o legales autorizados.

#### **Artículo 6º — Intercambio y reutilización de datos.**

1. El intercambio de datos entre organismos públicos o entre éstos y entidades privadas sólo podrá realizarse mediante convenios específicos, aprobados por la Autoridad de Protección de Datos.
2. Todo flujo de datos deberá quedar registrado en el Sistema Nacional de Interoperabilidad y Datos Públicos (SNIDP), creado por la presente ley, con registro de accesos, finalidad, fecha y organismo interviniente.
3. El intercambio se realizará mediante plataformas seguras, con cifrado extremo a extremo y protocolos de autenticación robustos.

#### **Artículo 7º — Sistema Nacional de Interoperabilidad y Datos Públicos (SNIDP).**

Créase el SNIDP, dependiente de la Autoridad Nacional de Ciberseguridad y Transformación Digital, con las siguientes funciones:

- a) Establecer estándares técnicos para la interoperabilidad de datos.
- b) Administrar el registro de accesos e intercambios de información.
- c) Coordinar la infraestructura de intercambio entre organismos públicos.
- d) Garantizar el principio de “solicitar solo una vez” mediante mecanismos automáticos de verificación.
- e) Supervisar el cumplimiento de las normas de seguridad, privacidad y ética en el tratamiento de datos públicos.

### **Capítulo III — Obligaciones y Derechos**

#### **Artículo 8° — Obligaciones de los responsables de datos.**

1. Cada organismo o entidad privada que trate datos personales deberá designar un Delegado de Protección de Datos (DPD).
2. El DPD será responsable de implementar políticas de privacidad, capacitar al personal y responder ante la autoridad de control.
3. Los sistemas deberán incluir funciones de auditoría, anonimización, revocación de consentimiento y reversión de datos inexactos.

#### **Artículo 9° — Derechos de las personas.**

Toda persona tiene derecho a:

- a) Acceder gratuitamente a sus datos personales en poder del Estado o de entidades privadas.
- b) Solicitar su rectificación, actualización, cancelación o portabilidad.
- c) Conocer la finalidad y el uso de los datos cedidos o compartidos.
- d) Oponerse al tratamiento de sus datos en los casos legalmente previstos.
- e) Solicitar la eliminación de datos que hayan sido obtenidos sin su consentimiento o que hayan perdido su finalidad legítima.

#### **Artículo 10° — Protección frente al fraude digital.**

1. En caso de utilización fraudulenta de datos personales o suplantación de identidad digital, el ciudadano tendrá derecho a la reversión inmediata de los efectos y a la restitución de fondos o derechos vulnerados.
2. Las entidades financieras, de pago o plataformas digitales serán solidariamente responsables en caso de incumplimiento de las medidas de autenticación seguras o de notificación de incidentes.
3. La Autoridad Nacional podrá ordenar medidas correctivas y sancionar con multas, suspensión de licencias o inhabilitación temporal.

## **Capítulo IV — Ética, Supervisión y Cooperación**

### **Artículo 11° — Gestión ética de los datos.**

Los organismos públicos y privados deberán adoptar códigos de ética, mecanismos de control y auditoría independientes en toda actividad de análisis de datos, inteligencia artificial o toma de decisiones automatizadas.

### **Artículo 12° — Supervisión y sanciones.**

La Autoridad Nacional de Ciberseguridad y Transformación Digital actuará en coordinación con la AAIP para supervisar el cumplimiento de las disposiciones de este Título, pudiendo aplicar:

- a) Multas graduables.
- b) Suspensión o cancelación de registros.
- c) Inhabilitación de funcionarios responsables por dolo o negligencia grave.

### **Artículo 13° — Cooperación internacional.**

La Autoridad Nacional coordinará acciones con organismos internacionales, en especial con el GAFI, la OCDE y la ONU, para alinear los estándares nacionales con las mejores prácticas globales sobre prevención del lavado de activos, financiación del terrorismo, privacidad y ciberseguridad.

## **Capítulo V — Disposiciones Complementarias**

### **Artículo 14° — Reglamentación.**

El Poder Ejecutivo Nacional reglamentará los estándares técnicos, plazos y procedimientos necesarios para la plena implementación del principio de solicitar solo una vez, en un plazo no mayor a 180 días.

# **TÍTULO III — INTELIGENCIA ARTIFICIAL EN POLÍTICAS PÚBLICAS**

### **Artículo 15° — Protección y tratamiento**

1. Toda recolección, almacenamiento, tratamiento o intercambio de datos personales por parte del Estado o de organizaciones privadas deberá realizarse conforme a los principios de licitud, finalidad, proporcionalidad, transparencia y minimización.

2. El intercambio de datos entre organismos públicos y privados requerirá bases legales claras y autorización de la autoridad competente.
3. Se promoverá la creación de un Registro Nacional de Intercambio de Datos Públicos y Privados, supervisado por la Autoridad de Protección de Datos.

#### **Artículo 16° — Gestión ética de los datos**

El Estado y las organizaciones deberán aplicar códigos de ética y mecanismos de rendición de cuentas para el uso de datos en políticas públicas, inteligencia artificial o analítica avanzada.

#### **Artículo 17° — Marco ético y regulatorio**

1. La utilización de sistemas de inteligencia artificial por parte del Estado deberá regirse por principios de legalidad, transparencia, no discriminación y supervisión humana.
2. Todo uso de IA en políticas públicas deberá ser auditável y sujeto a evaluación de impacto ético y social.
3. Se creará un Consejo Nacional de Ética e Inteligencia Artificial, de carácter consultivo y multiactor.

## **TÍTULO IV — IDENTIDAD DIGITAL Y DOCUMENTOS ELECTRÓNICOS**

#### **Artículo 18° — Identidad digital**

1. Se reconoce la identidad digital como equivalente funcional de la identidad física para actos jurídicos y relaciones con el Estado y entre particulares.
2. Los documentos electrónicos, las firmas electrónicas y digitales gozarán de validez jurídica plena respecto de sus soportes físicos.
3. La autenticación deberá cumplir con los niveles de aseguramiento definidos por la autoridad de aplicación.

#### **Artículo 19° — Derecho a reversión y reparación**

Toda persona usuaria que resulte víctima de fraude digital tendrá derecho a la reversión de operaciones indebidas y a la restitución inmediata de fondos o bienes, conforme a procedimientos reglamentados.

# **TÍTULO V- TELECOMUNICACIONES, ACCESO Y COMPETITIVIDAD TECNOLÓGICA**

## **Artículo 20º — Cobertura universal y calidad**

1. El Estado garantizará el acceso universal y de calidad a Internet.
2. Se establecerán estándares mínimos de calidad y continuidad para los servicios de telecomunicaciones y comercio electrónico.
3. Se promoverá la reducción de la brecha digital mediante inversiones y acuerdos público-privados.

## **Artículo 21º — Fomento de la industria tecnológica**

1. Se adaptarán los marcos regulatorios para incentivar la instalación de empresas tecnológicas internacionales y el desarrollo nacional.
2. El Estado facilitará la innovación mediante incentivos fiscales y acceso a financiamiento.
3. Se promoverán políticas para fortalecer la infraestructura digital, la ciberseguridad industrial y la formación de talento tecnológico.

# **TÍTULO VI — ECONOMÍA DIGITAL, COMERCIO Y CONSUMIDORES**

## **Artículo 22º — Comercio electrónico y consumidores**

1. El comercio electrónico, los servicios digitales, las plataformas de streaming y las aplicaciones deberán garantizar transparencia, seguridad y protección de los consumidores.
2. Se establecerán procedimientos rápidos de resolución de conflictos y reversión de cobros indebidos.
3. La publicidad digital deberá cumplir con criterios de veracidad y responsabilidad de las plataformas.

## **TÍTULO VII — TRABAJO, EDUCACIÓN Y SALUD DIGITALES**

### **Artículo 23º — Actualización de normas laborales**

1. El Estado promoverá la actualización del régimen laboral para incorporar el teletrabajo, la educación remota y los procesos médicos digitales, garantizando derechos laborales y privacidad.
2. Se impulsarán políticas para el desarrollo de competencias digitales en trabajadores, docentes y personal de salud.

## **TÍTULO VIII — COMPRAS PÚBLICAS E INNOVACIÓN**

### **Artículo 24º — Compras innovadoras**

1. El Estado actualizará la normativa de compras públicas para permitir modelos de riesgo compartido y fomentar la cooperación con startups y universidades.
2. Se regulará la propiedad intelectual de las innovaciones co-creadas con el Estado, asegurando el beneficio público y la transparencia de resultados.

## **TÍTULO IX — AUTORIDAD DE APLICACIÓN Y COORDINACIÓN**

### **Artículo 25º — Creación de la Autoridad Nacional de Ciberseguridad y Transformación Digital**

1. Créase la Autoridad Nacional de Ciberseguridad y Transformación Digital, organismo descentralizado con competencia en supervisar la ciberseguridad nacional, emitir estándares técnicos y coordinar políticas de datos e innovación.
2. Este organismo actuará en coordinación con la AAIP, BCRA, UIF, CNC y ARSAT.

## **TÍTULO X — DISPOSICIONES FINALES**

### **Artículo 26° — Reglamentación**

El Poder Ejecutivo Nacional reglamentará la presente ley en un plazo de 180 días desde su promulgación.

### **Artículo 27° — Compatibilidad internacional**

La presente ley se interpretará conforme a las Recomendaciones del GAFI, las normas ISO/IEC, las guías NIST y los acuerdos internacionales sobre cooperación digital.

## **TÍTULO XI — MARCO NACIONAL DE INTELIGENCIA ARTIFICIAL Y TRANSPARENCIA ALGORÍTMICA**

La inteligencia artificial (IA) y los algoritmos constituyen una de las transformaciones tecnológicas más profundas de nuestra era. En todo el mundo, los gobiernos y organismos internacionales —entre ellos Naciones Unidas, el G7, la OCDE y la Unión Europea—

han promovido principios éticos y marcos regulatorios destinados a garantizar que el desarrollo y uso de la IA se realice en forma transparente, segura y respetuosa de los derechos humanos.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea reconoce el derecho de las personas a no ser sometidas a decisiones exclusivamente automatizadas que afecten significativamente su vida. Francia, Reino Unido, Canadá, México y Australia, han adoptado estrategias nacionales con principios de explicabilidad, equidad, diversidad e inclusión en la investigación y el uso de la inteligencia artificial.

La República Argentina, comprometida con estos valores, establece en este Título el marco nacional para el desarrollo ético, responsable y transparente de la inteligencia artificial y los sistemas algorítmicos, promoviendo su uso para el bien común y evitando sesgos, discriminación o afectaciones indebidas a los derechos fundamentales.

### **Capítulo I — Principios Generales y Alcance**

#### **Artículo 28° — Objeto.**

El presente Título tiene por objeto establecer el marco jurídico, ético y operativo para el

desarrollo, implementación, supervisión y control de los sistemas de inteligencia artificial, aprendizaje automático y algoritmos automatizados en la República Argentina.

#### **Artículo 29° — Principios rectores.**

Toda aplicación de inteligencia artificial deberá ajustarse a los siguientes principios:

- a) Dignidad y autonomía humana.
- b) Justicia, equidad e inclusión.
- c) Transparencia, explicabilidad y trazabilidad de los procesos algorítmicos.
- d) Seguridad, protección de datos y privacidad.
- e) Supervisión humana significativa.
- f) Responsabilidad y rendición de cuentas.
- g) Sostenibilidad y proporcionalidad en el uso tecnológico.

#### **Artículo 30° — Derecho a la explicabilidad.**

Toda persona tendrá derecho a recibir información significativa sobre la lógica aplicada por un sistema algorítmico o automatizado que tenga efectos legales o significativos sobre su vida, así como las medidas de corrección o apelación disponibles.

### **Capítulo II — Evaluación Ética, Supervisión y Responsabilidad Algorítmica**

#### **Artículo 31° — Evaluación de impacto algorítmico.**

1. Todo organismo público o entidad privada que implemente sistemas de inteligencia artificial en procesos de decisión que afecten derechos, beneficios o servicios deberá realizar una Evaluación de Impacto Algorítmico (EIA).
2. La EIA deberá identificar los posibles riesgos éticos, sociales y de derechos humanos, y proponer medidas de mitigación.
3. Las EIA serán públicas y auditables por la Autoridad Nacional.

#### **Artículo 32° — Registro Nacional de Algoritmos de Alto Impacto (RNAI).**

Créase el RNAI, administrado por la Autoridad Nacional de Ciberseguridad y Transformación Digital, donde deberán inscribirse todos los algoritmos utilizados por el sector público y las empresas proveedoras de servicios digitales críticos. El registro incluirá la descripción funcional, finalidad, base de datos utilizada, mecanismos de supervisión y resultados de auditorías éticas.

**Artículo 33º — Supervisión humana obligatoria.**

Todo sistema algorítmico de impacto significativo deberá garantizar la posibilidad de revisión humana.

Las decisiones automatizadas en materia judicial, crediticia, sanitaria, laboral o educativa deberán contar con instancias humanas de validación, apelación o anulación.

**Artículo 34º — Responsabilidad.**

1. Los desarrolladores, proveedores y usuarios institucionales de sistemas de IA serán solidariamente responsables por los daños

que resulten de decisiones automatizadas contrarias a la ley, la ética o los derechos humanos.

2. Las plataformas digitales deberán informar de manera clara cuando se utilicen algoritmos de recomendación o priorización de contenido.

**Capítulo III — Agencia Nacional de Ética y Transparencia Algorítmica (ANETA)****Artículo 35º — Creación y funciones.**

Créase la Agencia Nacional de Ética y Transparencia Algorítmica (ANETA), como órgano autárquico dependiente de la Autoridad Nacional de Ciberseguridad y Transformación Digital, con las siguientes funciones:

- a) Auditarse sistemas algorítmicos y de inteligencia artificial en el ámbito público y privado.
- b) Emitir certificaciones de transparencia y ética algorítmica.
- c) Supervisar el cumplimiento de las Evaluaciones de Impacto Algorítmico.
- d) Coordinar la cooperación internacional en materia de inteligencia artificial y derechos digitales.
- e) Promover la capacitación y formación ética de los equipos de desarrollo.

**Artículo 36º — Comité de Ética Algorítmica.**

La ANETA contará con un Comité Asesor Multiactor integrado por representantes de universidades, sociedad civil, sector privado y organismos públicos, encargado de dictaminar sobre casos complejos o de alto impacto ético y de proponer actualizaciones normativas.

**Capítulo IV — Aplicaciones Sectoriales Prioritarias****Artículo 37º — Sector Salud.**

Los sistemas de IA aplicados a la salud deberán garantizar el consentimiento informado digital, la protección de datos clínicos

y la trazabilidad del uso de información médica, de conformidad con los principios de ética biomédica y la normativa internacional.

**Artículo 38° — Seguridad y reconocimiento facial.**

El uso de tecnologías de reconocimiento facial o biométrico deberá estar sujeto a autorización judicial, finalidad legítima, limitación temporal, proporcionalidad y auditorías periódicas. Se prohíbe su aplicación masiva o indiscriminada sin consentimiento.

**Artículo 39° — Educación, empleo y consumo.**

Los algoritmos utilizados en procesos educativos, de selección laboral o en plataformas de comercio electrónico deberán evitar discriminación, sesgos o manipulación de precios, garantizando la explicabilidad y el derecho al reclamo de los afectados.

**Capítulo V — Cooperación Internacional y Disposiciones Finales**

**Artículo 40° — Cooperación internacional.**

La República Argentina promoverá la cooperación en el marco de la ONU, la UNESCO, la OCDE, el GAFI y el G20 para desarrollar estándares éticos y técnicos en materia de inteligencia artificial, datos y derechos digitales.

**Artículo 41° — Reglamentación.**

El Poder Ejecutivo Nacional reglamentará la presente disposición en un plazo de ciento ochenta (180) días a partir de la entrada en vigencia de la ley.

# **TÍTULO XII - TELECOMUNICACIONES, CONECTIVIDAD Y DESARROLLO TECNOLÓGICO COMPETITIVO**

**Capítulo I — Principios y Objetivos Generales**

### **Artículo 42º — Objeto.**

El presente Título tiene por objeto regular el desarrollo, la gestión y la supervisión del sistema nacional de telecomunicaciones y conectividad, promoviendo la cobertura universal, la calidad del servicio, la competencia leal y la sostenibilidad ambiental.

### **Artículo 43º — Principios rectores.**

Las políticas de telecomunicaciones y conectividad se regirán por los siguientes principios:

- a) Universalidad: garantizar el acceso equitativo a los servicios de comunicación digital en todo el territorio nacional.
- b) Calidad y continuidad: asegurar estándares mínimos de prestación, sin interrupciones indebidas.
- c) Soberanía tecnológica: fomentar la producción nacional de tecnologías, componentes e infraestructura crítica.
- d) Ética y sostenibilidad: promover el uso responsable de los recursos naturales y la protección del medio ambiente.
- e) Innovación y competencia: impulsar el desarrollo científico, tecnológico y empresarial bajo condiciones de transparencia y equidad.

## **Capítulo II — Infraestructura, Acceso y Calidad del Servicio**

### **Artículo 44º — Cobertura universal.**

El Estado garantizará el acceso a Internet de banda ancha y servicios de telecomunicaciones a toda la población, con prioridad en zonas rurales, regiones de frontera y comunidades vulnerables, como política de inclusión digital.

### **Artículo 45º — Estándares mínimos de calidad.**

Las empresas prestadoras de servicios deberán cumplir con los estándares de calidad, velocidad, disponibilidad y atención al usuario que establezca la Autoridad Nacional de Telecomunicaciones y Conectividad Sostenible (ANTECOS).

### **Artículo 46º — Infraestructura compartida.**

Se promoverá el uso compartido de infraestructuras físicas y digitales entre operadores públicos y privados, a fin de optimizar recursos y evitar duplicaciones innecesarias, respetando criterios de seguridad y confidencialidad de la información.

## **Capítulo III — Promoción de la Innovación y la Competencia**

**Artículo 47º — Fomento a la innovación.**

El Estado impulsará programas de desarrollo tecnológico nacional orientados a la producción de hardware, software, componentes y servicios relacionados con la conectividad, priorizando la cooperación entre universidades, centros de investigación y empresas tecnológicas.

**Artículo 48º — Inversión responsable.**

Las inversiones nacionales y extranjeras en el sector deberán cumplir con los principios de sostenibilidad ambiental, respeto a los derechos digitales, ética empresarial y protección de los consumidores.

**Artículo 49º — Compras públicas innovadoras.**

Las entidades del sector público podrán realizar compras innovadoras y proyectos de riesgo compartido en materia tecnológica, priorizando la participación de empresas nacionales y startups que promuevan la innovación sostenible.

**Capítulo IV — Desarrollo Sostenible, Energía y Medio Ambiente****Artículo 50º — Eficiencia energética y transición verde.**

Las redes de telecomunicaciones, centros de datos y sistemas de almacenamiento digital deberán implementar tecnologías que minimicen el consumo energético y la emisión de gases de efecto invernadero, favoreciendo el uso de energías renovables y la economía circular.

**Artículo 51º — Evaluación ambiental digital.**

Los proyectos de infraestructura de telecomunicaciones estarán sujetos a evaluación de impacto ambiental digital, conforme a la legislación nacional vigente y a los compromisos internacionales en materia de sostenibilidad y cambio climático.

**Artículo 52º — Gestión de residuos tecnológicos.**

Las empresas proveedoras de servicios tecnológicos deberán establecer planes de recolección, reciclaje y disposición segura de equipos y componentes electrónicos, bajo supervisión de la autoridad competente.

**Capítulo V — Autoridad Nacional de Telecomunicaciones y Conectividad Sostenible (ANTECOS)****Artículo 53º — Creación y naturaleza.**

Créase la Autoridad Nacional de Telecomunicaciones y Conectividad Sostenible

(ANTECOS), como ente autárquico dependiente de la Autoridad Nacional de Ciberseguridad y Transformación Digital, con autonomía técnica y financiera.

**Artículo 54° — Funciones.**

ANTECOS tendrá las siguientes funciones:

- a) Regular, supervisar y fiscalizar los servicios de telecomunicaciones y conectividad.
- b) Establecer estándares mínimos de calidad y sostenibilidad en la infraestructura tecnológica.
- c) Coordinar el despliegue de redes nacionales y regionales.
- d) Fomentar la investigación, la innovación y la transferencia tecnológica.
- e) Controlar el cumplimiento de los compromisos ambientales y energéticos del sector.
- f) Administrar el Fondo Nacional de Conectividad y Sostenibilidad Digital.

**Artículo 55° — Fondo Nacional de Conectividad y Sostenibilidad Digital.**

Créase el Fondo Nacional de Conectividad y Sostenibilidad Digital, destinado a financiar proyectos de expansión de redes, innovación tecnológica, transición energética y programas de inclusión digital en zonas rurales o de baja densidad poblacional.

**Artículo 56° — Participación ciudadana.**

ANTECOS deberá garantizar mecanismos de consulta pública, acceso a la información y participación ciudadana en los procesos de planificación y evaluación de políticas de telecomunicaciones.

**Capítulo VI — Cooperación Internacional y Disposiciones Finales**

**Artículo 57° — Cooperación internacional.**

La República Argentina promoverá la cooperación bilateral y multilateral con organismos internacionales, regionales y técnicos, a fin de impulsar la interoperabilidad, la innovación y la sostenibilidad en el ámbito de las telecomunicaciones y la conectividad.

**Artículo 58° — Reglamentación.**

El Poder Ejecutivo Nacional reglamentará la presente disposición en un plazo máximo de ciento ochenta (180) días a partir de su promulgación.

**TÍTULO XIII — ECONOMÍA**

# **DIGITAL, COMERCIO ELECTRÓNICO Y PROTECCIÓN DEL CONSUMIDOR**

El crecimiento de la economía digital en la República Argentina requiere la consolidación de un marco legal que proteja a los consumidores, fomente la confianza en las transacciones electrónicas, prevenga fraudes y asegure la trazabilidad y transparencia de las operaciones.

Este Título establece derechos, obligaciones y estándares éticos para los actores del ecosistema digital, promoviendo un entorno comercial seguro, responsable y sostenible, en armonía con las recomendaciones del Grupo de Acción Financiera Internacional (GAFI) y las políticas nacionales de ciberseguridad e identidad digital.

## **Capítulo I — Principios Generales y Derechos del Consumidor Digital**

### **Artículo 59° — Objeto.**

El presente Título regula el comercio electrónico, los servicios digitales y las transacciones financieras realizadas a través de medios electrónicos, garantizando la protección integral de los derechos de los consumidores y usuarios en el entorno digital.

### **Artículo 60° — Principios rectores.**

Las actividades comprendidas en la economía digital se regirán por los siguientes principios:

- a) Transparencia: toda oferta, publicidad o servicio digital deberá brindar información clara, completa y verificable.
- b) Seguridad: las transacciones deberán realizarse bajo estándares de protección de datos y autenticación reforzada.
- c) Responsabilidad solidaria: las plataformas intermediarias serán solidariamente responsables ante el consumidor por incumplimientos, fraudes o deficiencias del servicio.
- d) Reversibilidad: toda persona afectada por fraude, error o suplantación de identidad digital tendrá derecho a la reversión inmediata de pagos y la restitución de fondos.
- e) Trazabilidad: las operaciones digitales deberán registrar datos que permitan identificar el origen, destino y objeto de las transacciones.

### **Artículo 61º — Derechos del consumidor digital.**

El consumidor digital goza de los derechos establecidos en la Ley de Defensa del Consumidor y, además, de los siguientes:

- a) Derecho a la información clara y en lenguaje accesible sobre términos de uso, políticas de datos y precios.
- b) Derecho a la privacidad y protección de sus datos personales.
- c) Derecho a la asistencia y resolución eficaz ante reclamos electrónicos.
- d) Derecho a no ser sometido a decisiones automatizadas sin revisión humana.
- e) Derecho a recibir comprobantes electrónicos verificables de cada transacción.

## **Capítulo II — Comercio Electrónico y Plataformas Digitales**

### **Artículo 62º — Alcance.**

Quedan comprendidas las plataformas de comercio electrónico, aplicaciones móviles, servicios de streaming, redes sociales, marketplaces y cualquier otro entorno digital que medie o facilite la compra, venta o provisión de bienes y servicios dentro del territorio nacional.

### **Artículo 63º — Obligaciones de las plataformas.**

1. Las plataformas deberán garantizar mecanismos de atención y resolución de reclamos accesibles y en idioma español.
2. Deberán identificar de manera verificable a los vendedores o prestadores que operen en su espacio.
3. Están obligadas a conservar registros de transacciones por un período mínimo de cinco (5) años.
4. Serán solidariamente responsables por los daños causados por falta de diligencia, negligencia técnica o incumplimiento contractual.

### **Artículo 64º — Contratos digitales.**

Los contratos celebrados por medios electrónicos tendrán validez legal plena siempre que el consentimiento se exprese mediante mecanismos verificables de autenticación, firma electrónica o identidad digital reconocida.

## **Capítulo III — Pagos Electrónicos, Reversibilidad y Prevención de Fraudes**

### **Artículo 65º — Pagos digitales.**

Las entidades financieras, fintech y proveedores de servicios de pago deberán garantizar mecanismos de autenticación multifactor, notificación inmediata y trazabilidad en todas las operaciones electrónicas.

**Artículo 66° — Reversibilidad de operaciones.**

1. En caso de fraude, suplantación de identidad o error técnico, el usuario afectado tendrá derecho a la reversión automática de la operación.
2. La carga de la prueba recaerá sobre la entidad que reciba el reclamo, la cual deberá acreditar la autenticidad de la transacción.
3. La falta de respuesta en un plazo de diez (10) días hábiles implicará la aceptación del reclamo por silencio positivo.

**Artículo 67° — Prevención del lavado de dinero.**

Las plataformas, bancos y prestadores de servicios digitales deberán implementar sistemas de monitoreo y reporte de operaciones sospechosas, en cumplimiento de las recomendaciones del GAFI y de las normas de la Unidad de Información Financiera (UIF).

**Capítulo IV — Trazabilidad, Transparencia y Normas GAFI****Artículo 68° — Trazabilidad digital.**

Toda operación comercial o financiera realizada por medios electrónicos deberá contar con un registro digital auditabile que permita identificar la secuencia de intermediarios, instrumentos de pago y flujos financieros asociados.

**Artículo 69° — Intercambio de información y cooperación.**

La Autoridad Nacional de Ciberseguridad y Transformación Digital coordinará el intercambio de información con la UIF y el Banco Central de la República Argentina, a fin de garantizar la detección y mitigación de riesgos vinculados al fraude, el lavado de activos y la financiación del terrorismo.

**Capítulo V — Supervisión, Sanciones y Cooperación Internacional****Artículo 70° — Autoridad de aplicación.**

La Autoridad Nacional de Ciberseguridad y Transformación Digital, en coordinación con la Secretaría de Comercio Interior y la UIF, será responsable de la aplicación, fiscalización y sanción de las disposiciones del presente Título.

**Artículo 71° — Régimen sancionatorio.**

El incumplimiento de las obligaciones establecidas en la presente ley será sancionado

con:

- a) Apercibimiento o suspensión temporal de operaciones.
- b) Multas proporcionales al volumen de negocios.
- c) Inhabilitación temporal o definitiva para operar en el territorio nacional.
- d) Publicación obligatoria de las sanciones en medios digitales oficiales.

#### **Artículo 72º — Observatorio Nacional de Comercio y Derechos Digitales (ONCDD).**

Créase el Observatorio Nacional de Comercio y Derechos Digitales (ONCDD),

dependiente de la Autoridad Nacional de Ciberseguridad y

Transformación Digital, con las siguientes funciones:

- a) Monitorear las tendencias, riesgos y buenas prácticas del comercio digital.
- b) Emitir informes públicos anuales sobre cumplimiento, fraudes y reclamos.
- c) Proponer actualizaciones normativas y estándares de ética comercial digital.
- d) Promover la educación del consumidor en entornos electrónicos.

#### **Artículo 73º — Cooperación internacional.**

El Estado argentino fomentará la cooperación con organismos internacionales, regionales y financieros para fortalecer la trazabilidad,

la ética y la transparencia en las operaciones digitales, en consonancia con los estándares del GAFI, la OCDE y las Naciones Unidas.

#### **Artículo 74º — Reglamentación.**

El Poder Ejecutivo Nacional reglamentará la presente disposición en un plazo de ciento ochenta (180) días desde su promulgación.

## **TÍTULO XIV — DERECHOS LABORALES DIGITALES Y TELETRABAJO ÉTICO**

El avance de las tecnologías digitales ha transformado profundamente las relaciones laborales, generando nuevas oportunidades de empleo, formas de organización y desafíos en materia de derechos, equidad, inclusión y sostenibilidad. El presente Título establece los principios, garantías y mecanismos necesarios para asegurar un entorno de trabajo digital ético, digno y justo, que promueva tanto la protección de los trabajadores como la innovación y la competitividad nacional.

Se reconocen los derechos laborales en entornos digitales y se fomenta la creación de empleo tecnológico, la formación digital y el acceso equitativo a las oportunidades de trabajo remoto, tanto en el sector público como en el privado, incluyendo el trabajo transfronterizo y las plataformas digitales.

## **Capítulo I — Principios, Alcance y Derechos del Trabajador Digital**

### **Artículo 75º — Objeto.**

El presente Título tiene por objeto establecer el marco normativo para la regulación del trabajo digital, el teletrabajo y las nuevas modalidades de empleo tecnológico, garantizando los derechos laborales, la inclusión social y la equidad en el acceso a oportunidades digitales.

### **Artículo 76º — Principios rectores.**

Las políticas de trabajo digital se regirán por los siguientes principios:

- a) Dignidad humana y justicia social.
- b) Igualdad de oportunidades y no discriminación digital.
- c) Inclusión y capacitación tecnológica.
- d) Protección de la salud, la privacidad y los datos personales del trabajador.
- e) Equilibrio entre la vida laboral y personal.
- f) Promoción de la sostenibilidad y responsabilidad tecnológica.

### **Artículo 77º — Ámbito de aplicación.**

Las disposiciones del presente Título se aplican a toda forma de prestación laboral que utilice tecnologías digitales, incluyendo el teletrabajo, trabajo remoto, trabajo en plataformas digitales, empleo transfronterizo y modalidades híbridas, tanto en el sector público como en el privado.

## **Capítulo II — Teletrabajo Ético y Protección Laboral**

### **Artículo 78º — Condiciones laborales mínimas.**

Los trabajadores digitales gozarán de los mismos derechos y beneficios que los trabajadores presenciales, incluyendo remuneración justa, seguridad social, licencias, vacaciones, representación sindical y acceso a mecanismos de reclamo y mediación.

### **Artículo 79º — Derecho a la desconexión digital.**

Todo trabajador digital tendrá derecho a la desconexión fuera de su jornada laboral, sin ser objeto de sanciones, represalias o pérdida de

beneficios por no responder comunicaciones fuera del horario establecido. Los empleadores deberán respetar los tiempos de descanso, familia y ocio digitalmente libre.

#### **Artículo 80° — Seguridad y salud digital.**

Los empleadores deberán adoptar medidas técnicas, organizativas y formativas para prevenir riesgos psicosociales, ergonómicos y de sobrecarga digital. El Ministerio de Trabajo establecerá protocolos de bienestar digital y evaluación de riesgos tecnológicos.

### **Capítulo III — Plataformas, Freelancers y Empleo Transfronterizo**

#### **Artículo 81° — Transparencia algorítmica.**

Las plataformas digitales que asignen tareas o determinen ingresos mediante algoritmos deberán garantizar la transparencia de los criterios utilizados, el acceso del trabajador a información sobre su desempeño y la posibilidad de revisión humana de las decisiones automatizadas.

#### **Artículo 82° — Derechos de los trabajadores de plataformas.**

1. Las plataformas deberán registrar a los trabajadores que presten servicios de manera habitual o continua.
2. Deberán asegurar la cobertura de salud, seguridad social y mecanismos de contribución previsional.
3. Se reconocerá la relación laboral cuando exista dependencia económica o continuidad funcional, aun en entornos digitales.

#### **Artículo 83° — Empleo remoto transfronterizo.**

El trabajo remoto prestado desde la República Argentina para empleadores extranjeros deberá garantizar las mismas condiciones de protección social, derechos laborales y cumplimiento impositivo que las relaciones locales, salvo acuerdos bilaterales específicos.

### **Capítulo IV — Capacitación, Inclusión y Formación Tecnológica**

#### **Artículo 84° — Formación digital continua.**

El Estado promoverá programas de alfabetización y formación digital para trabajadores, emprendedores y funcionarios públicos, con el fin de reducir la brecha tecnológica y fomentar la empleabilidad en el ámbito digital.

#### **Artículo 85° — Incentivos a la reconversión laboral.**

Se crearán programas de capacitación para la reconversión de trabajadores hacia sectores tecnológicos, priorizando a jóvenes, mujeres, personas con discapacidad y sectores vulnerables.

**Artículo 86° — Alianzas público-privadas.**

El Ministerio de Trabajo, en coordinación con la Autoridad Nacional de Ciberseguridad y el sector privado, fomentará convenios para la formación en habilidades digitales, inteligencia artificial, ciberseguridad y economía del conocimiento.

**Capítulo V — Dirección Nacional de Trabajo Digital y Derechos Laborales Tecnológicos (DINTEL)**

**Artículo 87° — Creación.**

Créase la Dirección Nacional de Trabajo Digital y Derechos Laborales Tecnológicos (DINTEL), como organismo especializado dependiente del Ministerio de Trabajo, Empleo y Seguridad Social, con autonomía técnica y coordinada con la Autoridad Nacional de Ciberseguridad y Transformación Digital.

**Artículo 88° — Funciones.**

DINTEL tendrá las siguientes funciones:

- a) Supervisar las condiciones laborales en entornos digitales.
- b) Promover políticas de equidad, bienestar y salud digital.
- c) Fiscalizar el cumplimiento de los derechos laborales digitales.
- d) Mediar en conflictos entre plataformas y trabajadores.
- e) Emitir informes públicos anuales sobre el estado del trabajo digital en Argentina.
- f) Impulsar la cooperación internacional en materia de empleo digital y derechos tecnológicos.

**Capítulo VI — Disposiciones Finales**

**Artículo 89° — Coordinación institucional.**

El Ministerio de Trabajo coordinará con la Autoridad Nacional de Ciberseguridad, el Ministerio de Educación y el Ministerio de Ciencia, Tecnología e Innovación la ejecución de políticas conjuntas de empleo digital, educación tecnológica y ética del trabajo en entornos digitales.

**Artículo 90° — Reglamentación.**

El Poder Ejecutivo Nacional reglamentará la presente disposición en un plazo de ciento

ochenta (180) días desde su promulgación.

# **TÍTULO XV — GOBERNANZA DIGITAL Y COORDINACIÓN INTERINSTITUCIONAL**

El fortalecimiento del ecosistema digital nacional requiere una gobernanza moderna, transparente y participativa que asegure la coherencia entre políticas públicas, la cooperación entre los distintos niveles del Estado y la integración con el sector privado, académico y la sociedad civil. El presente Título establece el marco institucional para la coordinación interinstitucional en materia de ciberseguridad, transformación digital, inteligencia artificial, telecomunicaciones y economía digital.

## **Capítulo I — Principios y Objetivos de la Gobernanza Digital**

### **Artículo 91º — Objeto.**

El presente Título tiene por objeto establecer las bases de un sistema nacional de gobernanza digital que garantice la coordinación, transparencia y eficiencia en la implementación de políticas públicas en materia digital y tecnológica.

### **Artículo 92º — Principios rectores.**

Las acciones y decisiones del Sistema Nacional de Gobernanza Digital se regirán por los siguientes principios:

- a) Coordinación interinstitucional.
- b) Transparencia y rendición de cuentas.
- c) Federalismo cooperativo.
- d) Participación ciudadana y ética digital.
- e) Innovación y sostenibilidad tecnológica.
- f) Armonización normativa e interoperabilidad institucional.

### **Artículo 93º — Objetivos específicos.**

- a) Asegurar la coherencia entre las políticas de transformación digital y desarrollo tecnológico.

- b) Fortalecer la articulación entre organismos públicos nacionales, provinciales y municipales.
- c) Promover la integración entre Estado, sector privado, academia y sociedad civil.
- d) Impulsar la adopción de estándares internacionales en materia de seguridad, interoperabilidad y protección de datos.

## **Capítulo II — Sistema Nacional de Gobernanza Digital (SNGD)**

### **Artículo 94° — Creación.**

Créase el Sistema Nacional de Gobernanza Digital (SNGD), bajo la coordinación de la Autoridad Nacional de Ciberseguridad y Transformación Digital, con la participación de los ministerios, organismos descentralizados y entidades públicas que desarrollen políticas vinculadas a la economía digital, inteligencia artificial, innovación, telecomunicaciones y derechos digitales.

### **Artículo 95° — Funciones.**

El SNGD tendrá las siguientes funciones:

- a) Coordinar las políticas y estrategias digitales del Estado nacional.
- b) Evaluar la implementación de los programas y proyectos en materia digital.
- c) Armonizar marcos regulatorios entre jurisdicciones.
- d) Promover la cooperación público-privada en innovación y ciberseguridad.
- e) Emitir informes anuales de avance en materia de gobernanza y transformación digital.

## **Capítulo III — Consejo Federal de Transformación Digital y Ciberseguridad**

### **Artículo 96° — Creación.**

Créase el Consejo Federal de Transformación Digital y Ciberseguridad como órgano consultivo y de articulación entre el Estado Nacional, las provincias, la Ciudad Autónoma de Buenos Aires, los municipios, las universidades y la sociedad civil.

### **Artículo 97° — Integración.**

El Consejo Federal estará integrado por:

- a) Representantes de los ministerios nacionales con competencia en materia digital, tecnológica, educativa, económica y laboral.
- b) Representantes de las provincias y municipios designados por el Consejo Federal de Inversiones (CFI).
- c) Representantes del sistema universitario y científico nacional.
- d) Representantes del sector privado, gremial y organizaciones de la sociedad civil

vinculadas a la transformación digital.

**Artículo 98° — Funciones del Consejo.**

- a) Emitir recomendaciones sobre políticas de gobernanza digital, ciberseguridad y derechos digitales.
- b) Promover la cooperación técnica y el intercambio de buenas prácticas entre jurisdicciones.
- c) Facilitar la coordinación de programas de inclusión y alfabetización digital.
- d) Contribuir al seguimiento de los objetivos de desarrollo sostenible (ODS) en materia digital.

**Capítulo IV — Transparencia, Evaluación y Participación Ciudadana**

**Artículo 99° — Transparencia digital.**

Todos los organismos que integren el Sistema Nacional de Gobernanza Digital deberán publicar información actualizada sobre sus políticas, presupuestos, indicadores de gestión y evaluaciones de impacto en portales de acceso público.

**Artículo 100° — Participación ciudadana.**

Se garantizará la participación activa de la ciudadanía a través de consultas públicas, audiencias digitales y plataformas colaborativas para la elaboración y evaluación de políticas de transformación digital.

**Artículo 101° — Evaluación y auditoría.**

El Sistema Nacional de Gobernanza Digital deberá someterse a auditorías anuales de desempeño y transparencia, cuyos resultados serán publicados en el Boletín Oficial y en los portales institucionales correspondientes.

**Capítulo V — Disposiciones Finales y Transitorias**

**Artículo 102° — Armonización normativa.**

El Poder Ejecutivo Nacional promoverá la armonización de las normas nacionales, provinciales y municipales en materia de ciberseguridad, protección de datos, inteligencia artificial y telecomunicaciones, a fin de garantizar la coherencia del marco regulatorio.

**Artículo 103° — Cooperación internacional.**

La República Argentina fomentará la cooperación internacional en materia de gobernanza digital, transformación tecnológica, derechos

digitales y ciberseguridad, participando activamente en organismos multilaterales y acuerdos regionales.

**Artículo 104º — Entrada en vigencia.**

La presente ley entrará en vigencia a los noventa (90) días de su publicación en el Boletín Oficial. El Poder Ejecutivo Nacional deberá reglamentarla en un plazo máximo de ciento ochenta (180) días desde su promulgación.

**Firmado:**

**Natividad Vidal**

Autora del Proyecto

Capilla del Monte, Córdoba, Argentina

**Firma manuscrita digital:**



Natividad Vidal

DNI 27.716.481

**Correo institucional:**

[datosabiertossoberanosar@gmail.com](mailto:datosabiertossoberanosar@gmail.com)

**Acreditación:**

El presente proyecto es presentado en carácter de autora ciudadana y en cumplimiento de estándares internacionales de Gobierno Abierto, Transparencia Digital y Soberanía de Datos.

# **ANEXO I - INFRAESTRUCTURA CRÍTICA DIGITAL (ICD)**

## **Definición**

Se considera **Infraestructura Crítica Digital** a todo sistema, red, plataforma, servicio o base de datos cuya indisponibilidad, alteración o compromiso pueda afectar:

- a) la seguridad nacional,
- b) la estabilidad económica y financiera,
- c) la salud y seguridad de la población,
- d) la continuidad de servicios esenciales,
- e) la soberanía tecnológica y de datos.

## **Sectores comprendidos**

Se consideran Infraestructuras Críticas Digitales, entre otras:

- sistemas financieros y bancarios,
- telecomunicaciones y conectividad,
- energía, agua y transporte,
- salud y registros sanitarios,
- identidad digital y registros civiles,
- plataformas estatales de datos,
- centros de datos estratégicos,
- sistemas electorales y de justicia.

## **Obligaciones mínimas**

Los operadores de ICD deberán:

- a) implementar planes de seguridad y continuidad,
- b) realizar análisis de riesgo periódicos,
- c) adoptar estándares internacionales reconocidos,
- d) reportar incidentes relevantes,
- e) someterse a auditorías técnicas.

# **ANEXO II - NIVELES DE RIESGO CIBERNÉTICO Y CLASIFICACIÓN**

## **Clasificación por niveles**

Los sistemas se clasificarán en:

- **Nivel 1 (Crítico)**
- **Nivel 2 (Alto)**
- **Nivel 3 (Medio)**
- **Nivel 4 (Básico)**

La clasificación determinará exigencias técnicas y de control.

## **Criterios de clasificación**

Se evaluará:

- a) impacto potencial,
- b) volumen y sensibilidad de datos,
- c) dependencia sistémica,
- d) exposición a amenazas,
- e) capacidad de recuperación.

## **Revisión periódica**

La clasificación deberá revisarse al menos cada **24 meses** o ante cambios sustanciales.

# **ANEXO III - PROTOCOLOS DE INCIDENTES, RESPUESTA Y REVERSIÓN**

## **Incidente de ciberseguridad**

Se considera incidente todo evento que comprometa:

- confidencialidad,
- integridad,
- disponibilidad,
- autenticidad de sistemas o datos.

## **Notificación obligatoria**

Los incidentes relevantes deberán notificarse:

- a la autoridad competente,
- dentro de plazos definidos según nivel de riesgo,
- garantizando trazabilidad y registro.

## **Reversión y protección del usuario**

En casos de fraude digital o robo de identidad:

- a) se garantizará la reversión administrativa y técnica,
  - b) se protegerá a la persona afectada,
  - c) se preservará la prueba digital.
-

# **ANEXO IV - CERTIFICACIONES, ESTÁNDARES Y AUDITORÍAS**

## **Estándares reconocidos**

Se consideran estándares válidos, entre otros:

- ISO/IEC 27001,
- ISO 22301,
- NIST Cybersecurity Framework,
- estándares nacionales equivalentes.

## **Certificación progresiva**

La certificación será:

- gradual,
- proporcional al nivel de riesgo,
- obligatoria para infraestructuras críticas.

## **Auditorías**

Los sistemas estarán sujetos a:

- auditoría interna,
- auditoría independiente,
- control estatal.

Los resultados agregados deberán publicarse.

---

# **ANEXO V - COORDINACIÓN FEDERAL, COOPERACIÓN Y TRANSICIÓN**

## **Coordinación federal**

La implementación se realizará en coordinación con:

- provincias,
- municipios,
- universidades,
- sector científico-tecnológico.

## **Cooperación internacional**

La autoridad de aplicación promoverá cooperación con:

- organismos multilaterales,
- redes de respuesta a incidentes,
- sistemas de alerta temprana.

## **Régimen transitorio**

La adecuación a la ley será:

- progresiva,
- con plazos razonables,
- priorizando infraestructuras críticas.

# **CLÁUSULA DE ARTICULACIÓN Y COMPLEMENTARIEDAD NORMATIVA**

Las leyes que integran el **Marco Integral para la Soberanía Digital, la Transparencia Económica y la Transición Tecnológica Sostenible** se interpretarán y aplicarán de manera **armónica, sistemática y complementaria**, respetando la autonomía normativa de cada una de ellas y los principios constitucionales vigentes.

A los efectos de su implementación, las disposiciones contenidas en este Marco deberán coordinarse entre sí, priorizando la coherencia regulatoria, la interoperabilidad institucional, la eficiencia administrativa y la seguridad jurídica, sin que la aplicación de una norma implique la exclusión, derogación tácita o contradicción de las restantes, salvo disposición expresa en contrario.

Las autoridades de aplicación de las distintas leyes que conforman el presente Marco promoverán mecanismos de **cooperación interinstitucional, federal y multisectorial**, con el fin de asegurar una implementación progresiva, coordinada y eficaz, evitando superposiciones regulatorias y garantizando el cumplimiento de los objetivos estratégicos del Estado en materia de gobernanza de datos, transparencia económica, desarrollo tecnológico, sostenibilidad ambiental y seguridad digital.

Asimismo, las políticas, reglamentaciones y actos administrativos que se dicten en el marco de las leyes integrantes de este Marco deberán orientarse a fortalecer la **trazabilidad, la transparencia, la protección de derechos, la innovación responsable y la estabilidad sistemática**, como principios transversales de la acción estatal.

La presente cláusula tiene carácter interpretativo y orientador, y no altera el contenido, alcance ni vigencia individual de las leyes que integran el Marco Integral.