CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
RECIBIDO
PROYECTO DE LEY N°
13568/2025-CR RU 2165874
15 DICIEMBRE 2025 11:38 a. m.
FIRMADO DIGITALMENTE: EBOHORQUEZ

JHAKELINE KATY UGARTE MAMANI
Congresista de la República

"Año de la recuperación y consolidación de la economía peruana"

LEY QUE FORTALECE EL SISTEMA NACIONAL DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS Y LA DEFENSA DIGITAL DEL ESTADO

La congresista **JHAKELINE KATY UGARTE MAMANI**, integrante de la **bancada Juntos por el Perú - Voces del Pueblo - Bloque Magisterial,** ejerciendo el derecho de iniciativa legislativa que le confiere el artículo 107 de la Constitución Política del Perú y de conformidad con lo establecido en los artículos 22-C, 67, 75 y 76 del Reglamento del Congreso de la República, asimismo en vocación y respeto a su investidura parlamentaria establecido en los artículos 4.1, 4.2 del Reglamento de Código de Ética del Congreso de la República, presenta el siguiente:

El Congreso de la República;
Ha dado la Ley siguiente

FORMULA LEGAL

LEY QUE FORTALECE EL SISTEMA NACIONAL DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS Y LA DEFENSA DIGITAL DEL ESTADO

Artículo 1. Objeto y finalidad
La presente Ley tiene por objeto fortalecer el Sistema Nacional de Ciberseguridad para la protección de las infraestructuras críticas digitales y la defensa digital del Estado, estableciendo la gobernanza, obligaciones, estándares mínimos, mecanismos de coordinación interinstitucional, reporte de incidentes y régimen de supervisión y sanciones.

Artículo 2. Ámbito de aplicación

La Ley se aplica a:
(i) las entidades del Poder Ejecutivo, Legislativo, Judicial, organismos constitucionalmente autónomos, gobiernos regionales y locales;
(ii) los operadores de servicios esenciales en los sectores de energía, agua y saneamiento, telecomunicaciones, transporte, salud y sistema financiero;
(iii) los proveedores de servicios tecnológicos críticos que soporten a las entidades u operadores antes indicados;
(iv) toda persona jurídica que administre o explote infraestructura crítica digital designada por la autoridad competente.

Artículo 3. Definiciones
Para efectos de la presente Ley, se entiende por:

a) **Ciberseguridad:** Conjunto de medidas técnicas, organizativas y legales destinadas a

proteger la confidencialidad, integridad, disponibilidad y resiliencia de redes, sistemas y datos.
b) **Incidente de ciberseguridad**: Evento que compromete o puede comprometer la continuidad, confidencialidad o integridad de servicios o sistemas de información.
c) **Infraestructura crítica digital (ICD):** Activos, plataformas, aplicaciones o redes cuyo funcionamiento es esencial para la continuidad de servicios básicos o el funcionamiento del Estado, y cuya afectación tendría impacto severo en la seguridad nacional, la economía, la salud pública o el orden interno.
d) Operador de servicios esenciales: Persona jurídica pública o privada responsable de la provisión de un servicio cuya interrupción tendría efectos significativos en la sociedad.
e) Centro Nacional de Seguridad Digital (CNSD): Órgano técnico especializado de la PCM responsable de articular, coordinar y supervisar las políticas y acciones de ciberseguridad en el ámbito civil.
f) **Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT)**: Unidad técnica encargada de la prevención, detección y respuesta ante incidentes.
g) **Responsable de Seguridad Digital (CISO o equivalente)**: funcionario designado por cada entidad u operador para la gestión de la ciberseguridad y la coordinación con el CNSD.
h) **Plan de Seguridad Digital y Continuidad Operativa (PSDC)**: Documento que integra la gestión de riesgos, controles, contingencias y recuperación de desastres.

Artículo 4. Principios
La interpretación y aplicación de esta Ley se rige por los siguientes principios: a) Seguridad nacional; b) Prevención y resiliencia; c) Proporcionalidad y gradualidad; d) Coordinación y subsidiariedad; e) Responsabilidad del operador; f) Mejora continua y auditoría; g) Protección de datos personales y privacidad; h) Soberanía y confianza digital.

Artículo 5. Rectoría, autoridad competente y coordinación
La Presidencia del Consejo de Ministros (PCM), ejerce la rectoría del Sistema Nacional de Ciberseguridad a través del CNSD, que actúa como autoridad técnica competente. El CNSD coordina con el Ministerio de Defensa y el Ministerio del Interior cuando los incidentes comprometan la defensa o el orden interno.

Asimismo, articula con los organismos reguladores sectoriales para la implementación de estándares y la supervisión del cumplimiento.

Artículo 6. Estándares mínimos y obligaciones generales
Las entidades y operadores comprendidos deben:

a) Implementar un sistema de gestión de seguridad de la información basado en estándares internacionales (por ejemplo, ISO/IEC 27001 y equivalentes), o lineamientos que emita la PCM;
b) Elaborar y mantener actualizado su PSDC;
c) Designar un CISO o responsable equivalente;
d) Realizar evaluaciones de riesgo, pruebas de penetración o ejercicios de cibercrisis al

menos una vez por año;
e) Capacitar periódicamente al personal;
f) Incorporar cláusulas de ciberseguridad en la contratación pública y en la gestión de proveedores;
g) Adoptar arquitectura de seguridad por diseño y privacidad desde el diseño en sistemas críticos.

Artículo 7. Participación de los organismos reguladores en el Sistema Nacional de Ciberseguridad

7.1 Integración institucional.
Forman parte del Sistema Nacional de Ciberseguridad, en calidad de entidades de enlace sectorial, los organismos reguladores de servicios públicos e infraestructura estratégica, entre ellos:

- El Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN),
- El Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL),
- La Superintendencia Nacional de Servicios de Saneamiento (SUNASS),

7.2 La Superintendencia de Banca, Seguros y AFP (SBS), Y otros que, por la naturaleza de los servicios esenciales bajo su ámbito, sean incorporados mediante Decreto Supremo refrendado por la Presidencia del Consejo de Ministros.

Artículo 8. Creación y funciones del Consejo Nacional de Ciberseguridad

8.1 Creación y naturaleza.
Créase el **Consejo Nacional de Ciberseguridad (CONACIBER)** como órgano de coordinación estratégica, asesoramiento y articulación interinstitucional del **Sistema Nacional de Ciberseguridad**, dependiente de la **Presidencia del Consejo de Ministros (PCM)**.

El CONACIBER tiene carácter **permanente** y su finalidad es formular lineamientos, aprobar planes nacionales y supervisar la ejecución coordinada de políticas públicas en materia de ciberseguridad y protección de infraestructuras críticas de información.

8.2 Conformación.
El Consejo Nacional de Ciberseguridad está integrado por los siguientes miembros titulares o sus representantes acreditados:

a. La **Presidencia del Consejo de Ministros (PCM)**, quien lo preside y ejerce la Secretaría Técnica a través del **Centro Nacional de Seguridad Digital (CNSD)**.
b. El **Ministerio de Defensa (MINDEF)**.
c. El **Ministerio del Interior (MININTER)**.
d. El **Ministerio de Energía y Minas (MINEM)**.
e. El **Ministerio de Transportes y Comunicaciones (MTC)**.

f. El **Ministerio de Salud (MINSA)**.
g. El **Ministerio de Economía y Finanzas (MEF)**.
h. Los organismos reguladores de servicios públicos e infraestructura estratégica: **OSINERGMIN**, **OSIPTEL**, **SUNASS**, **SBS**.
i. Un (1) representante de la **Contraloría General de la República**, en calidad de veedor permanente.
j. Un (1) representante de las **universidades públicas y privadas** con programas de ingeniería informática o seguridad digital, designado mediante convocatoria pública del CONACIBER.

Mediante **Decreto Supremo** refrendado por la PCM se podrá incorporar a otros sectores o entidades cuya competencia esté vinculada con la gestión de riesgos en el ciberespacio o la protección de infraestructuras críticas.

8.3 Funciones del Consejo Nacional de Ciberseguridad.

a. Aprobar la **Estrategia Nacional de Ciberseguridad** y sus planes de acción.
b. Emitir **lineamientos técnicos** y estándares mínimos para la gestión de riesgos y la protección de infraestructuras críticas digitales.
c. Coordinar la **respuesta ante incidentes graves o de impacto nacional**, asegurando la interoperabilidad entre las entidades competentes.
d. Supervisar la implementación de políticas, planes y programas de ciberseguridad en el ámbito público y privado.
e. Promover la **formación de capacidades nacionales** en ciberdefensa, investigación, innovación y educación digital.
f. Evaluar periódicamente la eficacia de las medidas adoptadas y recomendar mejoras normativas o presupuestales.
g. Facilitar el **intercambio de información y cooperación internacional**, en coordinación con el Ministerio de Relaciones Exteriores, para el combate de amenazas cibernéticas globales.

8.4 Secretaría Técnica.

La Secretaría Técnica del Consejo Nacional de Ciberseguridad recae en el **Centro Nacional de Seguridad Digital (CNSD)** de la PCM, que actúa como órgano técnico-ejecutor y responsable del seguimiento de acuerdos, la administración del **Registro Nacional de Infraestructuras Críticas Digitales** y la articulación con los **CSIRT sectoriales**.

<u>Artículo 9.</u> Creación del Registro Nacional de Infraestructuras Críticas Digitales (RNICD)

9.1 Creación y finalidad.

Créase el **Registro Nacional de Infraestructuras Críticas Digitales (RNICD)**, bajo la administración del **Centro Nacional de Seguridad Digital (CNSD)** de la Presidencia del Consejo de Ministros.

El RNICD tiene por finalidad identificar, clasificar y mantener actualizado el inventario de los sistemas, servicios y activos tecnológicos cuya afectación, interrupción o destrucción tendría un **impacto severo en la seguridad nacional, la economía, la salud pública o el orden interno**.

9.2 Criterios de identificación.

Son considerados **infraestructuras críticas digitales**, aquellas instalaciones, plataformas o servicios que cumplan uno o más de los siguientes criterios:
a. **Esencialidad:** Su funcionamiento es indispensable para la continuidad de servicios básicos (energía, agua, telecomunicaciones, transporte, salud, finanzas, defensa, justicia).
b. **Interdependencia:** Su afectación puede provocar efectos en cadena o colapsos sistémicos en otros sectores.
c. **Impacto potencial:** Su indisponibilidad puede poner en riesgo la vida, la integridad de las personas, la seguridad nacional o el funcionamiento del Estado.
d. **Conectividad digital:** Poseen infraestructura tecnológica, redes o sistemas de información interconectados que pueden ser objeto de ciberataques o sabotajes.

9.3 Clasificación.

El CNSD, en coordinación con los organismos reguladores y las entidades competentes, clasifica las infraestructuras críticas digitales según su nivel de sensibilidad o impacto, en tres categorías:
a. **Críticas:** cuya afectación generaría una interrupción masiva del servicio esencial.
b. **Altamente sensibles:** cuya afectación compromete datos, comunicaciones o información estratégica.
c. **Sensibles:** cuya afectación produce perturbaciones localizadas o temporales.

9.4 Obligaciones de las entidades registradas.

Las entidades públicas o privadas designadas como operadoras de infraestructuras críticas digitales están obligadas a:
a. Elaborar y mantener actualizado un **Plan de Seguridad Digital y Continuidad Operativa (PSDC)** conforme a los estándares definidos por el CNSD.
b. Designar un **responsable de Seguridad Digital (CISO o equivalente)** que sirva como punto de contacto ante incidentes.
c. **Reportar los incidentes de ciberseguridad** graves o de impacto sectorial al CNSD dentro de las setenta y dos (72) horas de su detección.
d. Someterse a **auditorías periódicas de seguridad** coordinadas por el CNSD y su organismo regulador correspondiente.
e. Participar en los **ejercicios nacionales de ciberresiliencia** que convoque el Consejo Nacional de Ciberseguridad.

9.5 Confidencialidad y protección de la información.

La información contenida en el RNICD tiene carácter reservado y de acceso restringido, y solo podrá ser utilizada con fines de planificación, prevención, supervisión o respuesta

ante incidentes de seguridad digital.
Su divulgación no autorizada será considerada falta grave conforme a la legislación sobre seguridad y defensa nacional.

9.6 Reglamentación.
Mediante Decreto Supremo refrendado por la Presidencia del Consejo de ministros, se establecerán los procedimientos técnicos, plazos, mecanismos de registro y actualización del RNICD, así como los formatos de reporte y los protocolos de coordinación con los organismos reguladores.

Artículo 10. Régimen de notificación de incidentes de ciberseguridad

10.1 Obligación de notificación.
Todas las entidades públicas y privadas comprendidas en el ámbito de aplicación de la presente ley, en especial aquellas que administren o operen **infraestructuras críticas digitales**, están obligadas a **notificar al Centro Nacional de Seguridad Digital (CNSD)** los incidentes de ciberseguridad que afecten o puedan afectar de manera significativa la continuidad, confidencialidad o integridad de sus servicios o sistemas de información.

10.2 Plazos de reporte.
La notificación deberá efectuarse dentro de los siguientes plazos máximos contados desde la detección del incidente:
a. **Incidentes graves o de alto impacto nacional:** hasta **24 horas**.
b. **Incidentes significativos o de impacto sectorial:** hasta **72 horas**.
c. **Incidentes menores o de bajo impacto:** dentro de los **cinco (5) días hábiles** siguientes a su identificación.

En caso de incidentes graves, la notificación inicial podrá ser **preliminar**, y deberá complementarse con un informe técnico detallado en un plazo máximo de **diez (10) días hábiles**.

10.3 Canales y formatos.
El CNSD establecerá los **canales electrónicos seguros y formatos estandarizados** para la recepción, clasificación y gestión de los reportes de incidentes. Los organismos reguladores sectoriales podrán implementar plataformas de reporte propias, siempre que estén **interconectadas con el sistema nacional de alertas digitales** administrado por el CNSD.

10.4 Coordinación interinstitucional.
El CNSD comunicará oportunamente los incidentes de impacto sectorial a los organismos reguladores competentes, a fin de activar los protocolos de supervisión o contingencia correspondientes.

En el caso de incidentes que afecten la seguridad o defensa nacional, el CNSD deberá

informar de inmediato al **Ministerio de Defensa**, **Ministerio del Interior** y al **Comando Conjunto de las Fuerzas Armadas**.

10.5 Clasificación de severidad.

Mediante Decreto Supremo refrendado por la PCM se aprobará la **matriz nacional de clasificación de incidentes**, considerando criterios de:

a. Alcance (número de usuarios o sistemas afectados).
b. Duración o persistencia del ataque.
c. Naturaleza del vector de ataque (ransomware, DDoS, exfiltración, sabotaje, etc.).
d. Impacto económico y reputacional.
e. Riesgo de contagio a otros sectores.

10.6 Sanciones por incumplimiento.

El incumplimiento de la obligación de notificar los incidentes en los plazos o formas establecidos constituirá **infracción grave** y será sancionado conforme al régimen administrativo que emita la PCM, sin perjuicio de las responsabilidades civiles o penales que correspondan.

Los organismos reguladores sectoriales aplicarán las sanciones dentro del ámbito de su competencia, conforme a la coordinación establecida por el Consejo Nacional de Ciberseguridad.

10.7 Confidencialidad y uso de la información.

La información contenida en los reportes de incidentes tiene carácter **confidencial y reservado**, y solo podrá ser utilizada para fines de prevención, respuesta, mitigación y aprendizaje institucional.

Su uso indebido o divulgación no autorizada se sancionará conforme a la normativa sobre acceso a la información clasificada y protección de datos personales.

<u>Artículo 12.</u> Promoción, cooperación e investigación en ciberseguridad

12.1Promoción de capacidades nacionales.

El Estado, a través de la Presidencia del Consejo de Ministros, promueve la formación de capacidades técnicas, científicas y profesionales en ciberseguridad, inteligencia digital, análisis forense informático y resiliencia tecnológica.
Para este fin, se impulsa la creación de **programas de especialización, becas y centros de excelencia** en coordinación con las universidades públicas y privadas, el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (CONCYTEC) y los organismos internacionales de cooperación.

12.2Educación y cultura digital.

El Ministerio de Educación y el Ministerio de Trabajo y Promoción del Empleo, en coordinación con la PCM, incorporan en los currículos educativos y programas de

formación técnica contenidos orientados al uso seguro y responsable del entorno digital, la protección de datos personales y la prevención de delitos informáticos.

12.3 Investigación y desarrollo tecnológico.

El Estado fomenta la investigación aplicada en ciberseguridad mediante el Fondo Nacional para la Innovación y la Resiliencia Digital, destinado a proyectos que desarrollen soluciones nacionales en criptografía, detección temprana de amenazas, inteligencia artificial aplicada y protección de infraestructuras críticas.

12.4 Cooperación internacional.

El Ministerio de Relaciones Exteriores, en coordinación con la PCM y el CONACIBER, promoverá acuerdos de cooperación, intercambio de información y asistencia técnica con organismos multilaterales, redes internacionales de respuesta ante incidentes (CSIRT globales) y agencias homólogas extranjeras.

Dichos acuerdos deberán respetar los principios de soberanía digital, protección de datos personales y seguridad nacional.

12.5 Alianzas público-privadas.

El Estado fomenta la participación del sector privado, gremios empresariales y organizaciones de la sociedad civil en programas de prevención, capacitación y respuesta coordinada ante incidentes de ciberseguridad, bajo los lineamientos del Consejo Nacional de Ciberseguridad.

12.6 Informe anual.

El Centro Nacional de Seguridad Digital publicará un **Informe Anual de Estado de la Ciberseguridad en el Perú**, que contendrá:

a. Las estadísticas nacionales de incidentes reportados.
b. La evaluación del nivel de cumplimiento de las obligaciones de la presente ley.
c. Las recomendaciones estratégicas para el año siguiente. Si

Este informe será remitido al Congreso de la República dentro de los tres primeros meses de cada año.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Reglamentación

El Poder Ejecutivo, mediante **Decreto Supremo** refrendado por la **Presidencia del Consejo de Ministros**, aprueba el **Reglamento de la presente Ley** en un plazo no mayor de **ciento ochenta (180) días calendario** contados a partir de su entrada en vigencia. El Reglamento precisará los procedimientos técnicos para la identificación de infraestructuras críticas digitales, los formatos de reporte de incidentes, los mecanismos de coordinación interinstitucional y los estándares mínimos de seguridad aplicables a los operadores de servicios esenciales.

Segunda. Creación del Fondo Nacional para la Resiliencia Digital

Créase el Fondo Nacional para la Resiliencia Digital (FONRED), bajo la administración de la Presidencia del Consejo de Ministros, destinado a financiar:

a. Proyectos de fortalecimiento de ciberseguridad en entidades públicas y empresas operadoras de infraestructuras críticas.
b. Programas de investigación, innovación y capacitación en ciberseguridad.
c. Acciones de respuesta inmediata ante incidentes de alto impacto.
El Fondo se constituye con recursos del presupuesto público, cooperación internacional no reembolsable y aportes del sector privado conforme a reglamento.

Tercera. Articulación con el Sistema Nacional de Defensa Civil y el SINAGERD

El **Consejo Nacional de Ciberseguridad** coordina con el **Instituto Nacional de Defensa Civil (INDECI)** y el **Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD)** las acciones de prevención, mitigación y recuperación frente a incidentes cibernéticos que afecten la continuidad de los servicios esenciales o pongan en riesgo la seguridad de la población.

Cuarta. Coordinación con el Sistema Nacional de Inteligencia

El **Centro Nacional de Seguridad Digital (CNSD)** establecerá mecanismos de intercambio seguro de información con los órganos del **Sistema Nacional de Inteligencia (SINA)**, conforme a la Ley N.° 28664, para la detección temprana de amenazas cibernéticas, asegurando el respeto a los principios de confidencialidad, legalidad y proporcionalidad.

Quinta. Informe anual al Congreso de la República
El Consejo Nacional de Ciberseguridad (CONACIBER) presentará anualmente al Congreso de la República un Informe de Resultados y Recomendaciones Estratégicas, que incluirá:

- El número de incidentes registrados y su impacto económico y operativo.
- Las medidas correctivas adoptadas.
- Las necesidades presupuestales para fortalecer la resiliencia digital del país.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

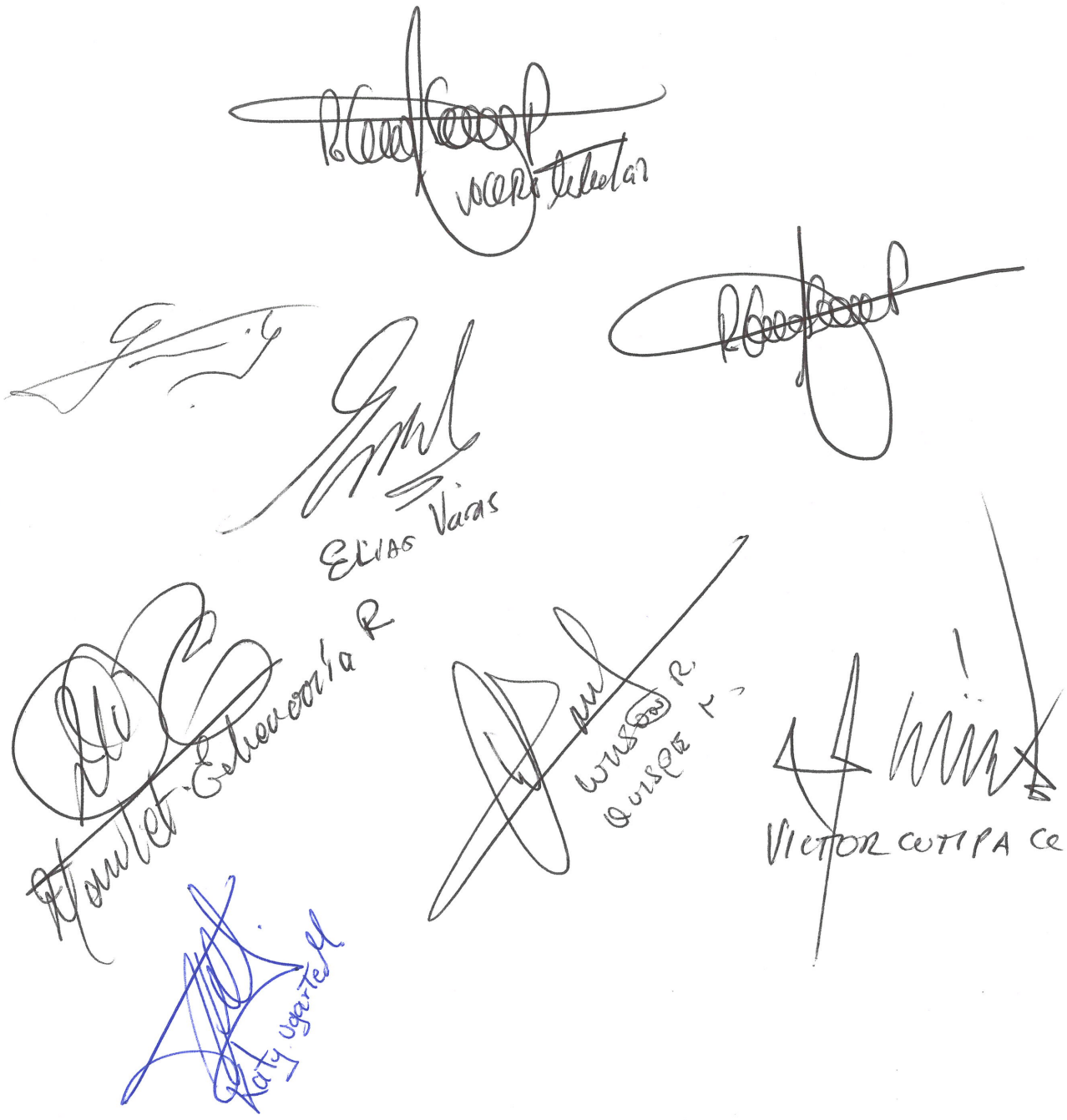
Primera. Adecuación progresiva de las entidades
Las entidades públicas y privadas que administren o gestionen infraestructuras críticas digitales dispondrán de un plazo máximo de **doce (12) meses** contados desde la entrada en vigencia del reglamento de la presente ley, para adecuar sus sistemas, políticas internas y planes de seguridad a las disposiciones aquí establecidas.

Segunda. Instalación del Consejo Nacional de Ciberseguridad

El **Consejo Nacional de Ciberseguridad (CONACIBER)** se instalará dentro de los **noventa (90) días calendario** siguientes a la publicación del reglamento de la presente ley, bajo convocatoria de la **Presidencia del Consejo de Ministros**.

Tercera. Plan de transición

Mientras se implementan el **Registro Nacional de Infraestructuras Críticas Digitales (RNICD)** y el **Fondo Nacional para la Resiliencia Digital (FONRED)**, el **Centro Nacional de Seguridad Digital (CNSD)** continuará ejerciendo las funciones de identificación, monitoreo y coordinación intersectorial, con cargo a su presupuesto institucional.



EXPOSICIÓN DE MOTIVOS

I. ANTECEDENTES

En los últimos años, el Perú ha experimentado un incremento sin precedentes en los ataques de ciberseguridad dirigidos contra entidades públicas, empresas estratégicas y operadores de servicios esenciales. Según los reportes de Fortinet (FortiGuard Labs), en 2024 se registraron 45,5 mil millones de intentos de ciberataques. Durante el primer semestre de 2025, se detectaron 748 millones adicionales, afectando principalmente a los sectores de energía, salud, telecomunicaciones, banca y servicios gubernamentales.

A nivel estatal, el Centro Nacional de Seguridad Digital (CNSD), adscrito a la PCM, ha gestionado más de 106 mil alertas de seguridad digital y coordina con 397 entidades de la Red Nacional CSIRT. Pese a ello, las capacidades institucionales son insuficientes frente al crecimiento y sofisticación de las amenazas.

Diversos incidentes recientes han comprometido información y servicios esenciales, como los ataques al MINSA (2022 y 2025), CENFOTUR (2024), Interbank (2024) y Banco de la Nación (2025), evidenciando vulnerabilidades graves en la infraestructura crítica digital del país.

Si bien existen normas como la Ley 30999, el DU 007-2020 o la Norma SBS 504-2021, ninguna establece un marco integral obligatorio que articule obligaciones técnicas, mecanismos de reporte, supervisión sectorial, protección de infraestructuras críticas y un régimen sancionador.

A nivel internacional, modelos como la Directiva NIS2 (UE), el Esquema Nacional de Seguridad (España), la CISA Act (EE.UU.) y la Ley 21.663 de Chile demuestran que la protección digital debe ser parte de la seguridad nacional.

II. OBJETIVO DE LA INICIATIVA

El proyecto tiene por objeto fortalecer el Sistema Nacional de Ciberseguridad, estableciendo un marco legal integral para la protección de infraestructuras críticas digitales y la defensa digital del Estado, mediante:

- La creación del Consejo Nacional de Ciberseguridad (CONACIBER) como instancia de coordinación multisectorial.
- El Registro Nacional de Infraestructuras Críticas Digitales (RNICD).
- La notificación obligatoria y clasificación de incidentes de ciberseguridad.
- La participación de los organismos reguladores (OSINERGMIN, OSIPTEL, SUNASS, SBS).
- La implementación de un régimen de sanciones y medidas correctivas.
- La creación del Fondo Nacional para la Resiliencia Digital (FONRED).

III. MARCO NORMATIVO

3.1 La propuesta se sustenta en los siguientes marcos constitucionales y legales:

- Constitución Política del Perú: Artículos 44 y 163 establecen que la defensa nacional y la seguridad del Estado son deberes fundamentales.
- Ley N.º 29158 – Ley Orgánica del Poder Ejecutivo, que faculta a la PCM a coordinar el Sistema Nacional de Seguridad.
- Ley N.º 30999 – Ley de Ciberdefensa, que regula la acción militar en el ciberespacio.
- Decreto de Urgencia N.º 007-2020, que crea el Centro Nacional de Seguridad Digital.
- Ley N.º 28664 – Ley del Sistema Nacional de Inteligencia, que permite el intercambio de información estratégica.
- Ley N.º 29733 – Ley de Protección de Datos Personales, que resguarda la privacidad en entornos digitales.

Asimismo, se inspira en las directrices internacionales y estándares como la Directiva NIS2 (UE 2022/2555), la Ley 21.663 de Chile (2024) y la CISA Act (EE. UU. 2018), que reconocen la ciberseguridad como parte de la seguridad nacional integral.

3.2 Legislación comparada

Diversos países han incorporado marcos normativos específicos:

España

La Ley 8/2011, de Protección de Infraestructuras Críticas, y su Real Decreto 43/2021, regulan las medidas de seguridad de las redes y sistemas de información. España cuenta además con el Esquema Nacional de Seguridad (ENS), que establece principios y requisitos mínimos de protección para toda la administración pública y empresas proveedoras de servicios esenciales.
Su modelo se basa en tres pilares:

- identificación de infraestructuras críticas;
- coordinación entre el Ministerio del Interior y el Centro Criptológico Nacional;
- y obligaciones de reporte inmediato de incidentes.

Relevancia para el Perú: muestra cómo una ley específica puede vincular defensa, interior y administración digital bajo un mismo sistema operativo nacional.

Estados Unidos

La Cybersecurity and Infrastructure Security Agency (CISA), creada por la Ley de Ciberseguridad e Infraestructura (2018), coordina la protección de infraestructuras críticas nacionales, con facultades para:

- emitir alertas y estándares obligatorios,
- exigir planes de contingencia,
- y coordinar con los sectores de energía, transporte y comunicaciones.

Además, el National Cybersecurity Protection Act (2014) promueve la colaboración público-privada para la respuesta ante incidentes y ciberataques.

Relevancia para el Perú: este modelo demuestra que la ciberseguridad debe gestionarse como parte de la seguridad nacional, no solo tecnológica, incluyendo la protección de sectores críticos y la inteligencia preventiva.

Unión Europea

La Directiva (UE) 2022/2555 (NIS2), vigente desde 2023, establece obligaciones a los Estados miembros para:

- adoptar estrategias nacionales de ciberseguridad;
- crear autoridades competentes y CSIRTs nacionales;
- imponer sanciones a entidades que no reporten incidentes graves;
- y asegurar la cooperación transfronteriza.

Relevancia para el Perú: ofrece un marco de gobernanza que podría inspirar un Sistema Nacional de Ciberseguridad con competencias claras, responsabilidades compartidas y un régimen sancionador escalonado.

Chile

La Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (Ley N° 21.663, 2024) crea la Agencia Nacional de Ciberseguridad, con funciones de supervisión, fiscalización y respuesta a incidentes.
Dispone la obligación de que las instituciones públicas y empresas estratégicas implementen planes de ciberseguridad y reporten eventos al Centro de Respuesta ante Incidentes (CSIRT Nacional).

Relevancia para el Perú: Chile ha logrado integrar la protección digital dentro de su estrategia nacional de defensa y soberanía tecnológica, un precedente directo aplicable a nuestra realidad.

Colombia

El CONPES 3854 (2016) aprobó la Política Nacional de Seguridad Digital, y en 2023 el país avanza hacia una Ley Integral de Ciberseguridad y Ciberdefensa.

El enfoque colombiano prioriza la cooperación interinstitucional y la formación de capacidades en los sectores de defensa, justicia y educación.

3.3 Relevancia para el Perú

Su enfoque muestra cómo se puede institucionalizar la ciberseguridad en todo el aparato estatal, con un componente educativo y de responsabilidad compartida.

País	Norma	Características relevantes
España	Ley 8/2011 yRD 43/2021	Define infraestructuras críticas y el Esquema Nacional de Seguridad (ENS).
Estados Unidos	CISA Act (2018)	Crea la agencia nacional para protección de infraestructuras críticas.
Unión Europea	Directiva NIS2 (2022)	Obliga a los Estados miembros a crear marcos nacionales y sanciones.
Chile	Ley 21.663 (2024)	Crea la Agencia Nacional de Ciberseguridad y regula los operadores esenciales.
Colombia	CONPES 3854 y Proyecto de Ley 2023	Integra defensa, justicia y educación digital en una política nacional.

Estos modelos destacan la necesidad de una gobernanza intersectorial, con participación de reguladores y plazos de notificación obligatoria, enfoque adoptado en el presente proyecto.

Las experiencias de España, Estados Unidos, la Unión Europea, Chile y Colombia coinciden en que:

- la ciberseguridad es un asunto de seguridad nacional;
- debe existir un marco legal con obligaciones claras, una autoridad competente y un sistema de respuesta ante incidentes;
- la coordinación público-privada y la protección de infraestructuras críticas son ejes esenciales;
- y la educación digital y la formación de capacidades técnicas son complementos estratégicos.

IV PROBLEMA PUBLICO IDENTIFICADO

El Perú carece de un marco legal integral para proteger eficazmente las infraestructuras críticas digitales y garantizar la seguridad digital del Estado, generando riesgos para la continuidad de los servicios esenciales y la confianza ciudadana.

Las normas vigentes como la Ley N.º 30999 de Ciberdefensa (de carácter militar) y el Decreto de Urgencia N.º 007-2020 que crea el CNSD— se limitan a la defensa nacional o a aspectos organizativos, sin establecer estándares vinculantes, régimen sancionador ni participación de los organismos reguladores.

Los incidentes que afectaron a entidades como el MINSA, CENFOTUR, Interbank y el Banco de la Nación demuestran que las vulnerabilidades tecnológicas pueden comprometer la continuidad de servicios esenciales y la confianza ciudadana en el Estado digital.

El proyecto busca alinearse con estos estándares, adaptándolos al contexto nacional mediante el fortalecimiento del Centro Nacional de Seguridad Digital, la creación de un registro de infraestructuras críticas y la coordinación con el Comando Conjunto de las Fuerzas Armadas y el Ministerio del Interior en materia de defensa digital.

Aquí demostramos los intentos de ciberataques en Perú (Fortinet)

- 2021: 11,5 mil millones de intentos.
- 2022: 15 mil millones (↑35% vs. 2021).
- 2023: 5 mil millones (cifra anual reportada por Fortinet para Perú).
- 2024: 45,5 mil millones (récord anual).
- 2025 (1er semestre): 748,2 millones (dato semestral; no anualizado).

Fortinet mide intentos/detecciones en su red de sensores. Las variaciones interanuales (por ejemplo, la caída 2023 y el salto 2024) pueden reflejar cambios en tácticas de ataque, cobertura de sensores y clasificación de eventos. 2025 es parcial (H1), por eso luce bajo frente a 2024.

Indicador estatal complementario (PCM – Centro Nacional de Seguridad Digital)

- Alertas de seguridad digital gestionadas por el CNSD (acumulado a 01/10/2025): 106.187 alertas; 397 entidades en la Red Nacional CSIRT. (Mide eventos gestionados por el Estado, no "intentos").

Perú — Ataques y destinatarios (sector / entidad)

Año	Sector objetivo	Entidad/ámbito (ejemplos)	Tipo de incidente (resumen)	Fuente
2022	Salud (sector público)	MINSA (base de datos de 44 mil usuarios)	Exfiltración de datos / venta en foros, alertado por PCM	conexionvida.pe
2024	Financiero (sistema supervisado)	Sistema financiero peruano (3 ataques confirmados por SBS)	Ciberataques diversos (no detallados públicamente por entidad)	El Comercio Perú
2024	Educación / Turismo (sector público)	CENFOTUR (Mincetur)	Ransomware que cifró redes; comunicado oficial	Gobierno del Perú
2024	Financiero (banca privada)	Interbank	Incidente de exposición de datos de clientes (divulgado públicamente)	infobae
2025 (jun.)	Financiero (banca estatal)	Banco de la Nación	Presunta filtración (el banco niega vulneración; investigación en curso en prensa)	infobae+1
2025 (sep.)	Salud (sector público)	MINSA – SIMEPLANS	Acceso no autorizado a plataforma administrativa (sin afectación a historias clínicas, según notas)	

Contexto sectorial adicional (LatAm/Global): Fortinet reporta en 2024 mayor presión sobre manufactura, servicios empresariales, construcción y retail (no desagregado para Perú); Microsoft y ESET muestran que salud y gobierno están entre los más atacados a nivel regional/global. Útil como benchmark cuando el reporte peruano no desagrega por sector.

- Finanzas: 2024 registró 3 ataques al sistema financiero (confirmado por SBS). Casos mediáticos incluyen Interbank 2024 y la presunta filtración en Banco de la Nación 2025 (la entidad la niega). Banco de la Nación+3El Comercio Perú+3infobae+3
- Salud: Eventos 2022 (MINSA) y 2025 (SIMEPLANS) muestran que el sector salud sigue bajo presión por ransomware/exfiltración. conexionvida.pe+1
- Entidades públicas: CENFOTUR comunicó ransomware (2024), evidenciando exposición de organismos del Estado. Gobierno del Perú

V ANALISIS SOBRE LA NECESIDAD, VIABILIDAD Y OPORTUNIDAD DE LA PROPUESTA

4.1. Necesidad de la propuesta

La presente iniciativa legislativa es necesaria porque el Perú enfrenta un escenario de amenazas cibernéticas crecientes que comprometen la continuidad de los servicios esenciales, la integridad de la información pública y privada, y la confianza ciudadana en el Estado digital.

Actualmente, el país carece de un marco legal integral que:

- defina y proteja formalmente las infraestructuras críticas digitales,
- establezca obligaciones técnicas exigibles a entidades públicas y operadores de servicios esenciales,
- disponga la notificación obligatoria de incidentes,
- articule a los organismos reguladores sectoriales en un mismo sistema nacional de ciberseguridad, y
- habilite un régimen sancionador por incumplimiento.

Las normas hoy vigentes —Ley N.° 30999 (ciberdefensa), DU N.° 007-2020 (CNSD) y regulaciones sectoriales dispersas— resultan insuficientes para enfrentar la magnitud, sofisticación y persistencia de las amenazas cibernéticas actuales.

4.2. Viabilidad de la propuesta

La propuesta es plenamente viable en términos institucionales, técnicos, jurídicos y presupuestales.

a. Viabilidad institucional

El país ya cuenta con estructuras que pueden ser fortalecidas e interconectadas: CNSD, Red Nacional CSIRT, organismos reguladores (OSIPTEL, OSINERGMIN, SUNASS, SBS) y sectores estratégicos con unidades de TI. La propuesta no crea nuevas entidades complejas, sino que articula las existentes.

b. Viabilidad jurídica

La Constitución y la Ley Orgánica del Poder Ejecutivo facultan a la PCM a coordinar sistemas nacionales. La iniciativa complementa y ordena el marco existente sin contradecir competencias legales.

c. Viabilidad técnica

Las medidas se basan en estándares internacionales: ISO 27001, Directiva NIS2, ENS, CISA Act, Ley 21.663 de Chile, lo que asegura una implementación factible y probada.

d. Viabilidad económica

La propuesta no genera gasto público significativo. Se crea el Fondo Nacional para la Resiliencia Digital (FONRED) sin afectar el Erario, aprovechando recursos existentes y cooperación internacional.

4.3 Oportunidad de la propuesta

a. Contexto nacional crítico

El aumento drástico de ciberataques (45,5 mil millones en 2024) demuestra la urgencia de normas obligatorias que fortalezcan la resiliencia del país.

b. Transformación digital del Estado

El Perú avanza hacia servicios digitales en salud, justicia, educación y banca. Sin un marco de ciberseguridad moderno, la digitalización estatal se vuelve vulnerable.

c. Alineamiento con estándares internacionales

La propuesta permite que el país se alinee con la Directiva NIS2, la CISA Act y marcos regionales, fortaleciendo la cooperación internacional y la confianza de operadores esenciales.

V. EFECTO DE LA NORMA PROPUESTA SOBRE LA LEGISLACIÓN NACIONAL

La propuesta legislativa busca Incorporar un enfoque integral e intersectorial, que abarca tanto el sector público como privado. En ese sentido, la presente iniciativa legislativa, no plantea la modificación de la legislación; y se encuentra enmarcada dentro de los alcances establecidos en la Constitución Política del Perú y las leyes de la materia, cumpliendo con lo establecido en el Reglamento del Congreso de la República.

VI. VINCULACIÓN AL ACUERDO NACIONAL

La presente iniciativa legislativa se encuentra vinculada y en armonía con las Políticas de Estado expresadas en el Acuerdo Nacional, específicamente; **I. Democracia y Estado de Derecho**, 7. erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana 9. política de seguridad nacional, **III. competitividad del país** 20. desarrollo de la ciencia y la tecnología