# PROYECTO DE LEY QUE DECLARA EL 3 DE DICIEMBRE DE CADA AÑO, COMO EL "DÍA NACIONAL DE LA CIBERSEGURIDAD"

El congresista de la república **ALFREDO PARIONA SINCHE**, miembro de la BANCADA SOCIALISTA, ejerciendo el derecho de iniciativa legislativa que le confiere el artículo 107 de la Constitución Política del Perú y en concordancia con los artículos 22 inciso c) 67, 75 y 76 del reglamento del Congreso de la República presenta el siguiente proyecto de ley.

## FÓRMULA LEGAL

El Congreso de la República,
Ha dado la ley siguiente:

## LEY QUE DECLARA EL 3 DE DICIEMBRE DE CADA AÑO, COMO EL "DÍA NACIONAL DE LA CIBERSEGURIDAD"

### Artículo 1. Objeto de la ley

La presente ley tiene por objeto declarar el día 3 de diciembre de cada año, como el "Día Nacional de la Ciberseguridad", con el propósito de promover la protección de los datos personales, la integridad de las infraestructuras digitales y, la confianza en el uso de las tecnologías de la información y la comunicación (TIC), a fin de concientizar, fortalecer las capacidades técnicas y educativas, fomentar la cooperación público-privada y, fomentar la investigación y la innovación en materia de ciberseguridad.

### Artículo 2. Declaratoria

Se declara el día 3 de diciembre de cada año, como el "Día Nacional de la Ciberseguridad".

### Artículo 3. Implementación

La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital, coordina con los ministerios, así como, con los sectores público y privado, la realización de las siguientes acciones:

a) Campañas nacionales de sensibilización sobre buenas prácticas digitales.
b) Simulacros nacionales de ciberataques orientados a mejorar la capacidad de respuesta institucional.

c) Programas educativos en coordinación con el Ministerio de Educación (Minedu) y la Autoridad Nacional del Servicio Civil (Servir), para incluir contenidos de ciberseguridad en todos los niveles de enseñanza y capacitación pública.
d) Reconocimiento anual "Perú Ciberseguro", a las instituciones que demuestren buenas prácticas y políticas efectivas de ciberseguridad.

**Artículo 4. Participación interinstitucional**

Las entidades públicas, empresas privadas, universidades y, organizaciones civiles participarán en las actividades del "Día Nacional de la Ciberseguridad", en el marco de la Política Nacional de Transformación Digital.

## DISPOSICIONES COMPLEMENTARIAS FINALES

**PRIMERA.** La Secretaría de Gobierno y Transformación Digital, en coordinación con la Presidencia del Consejo de Ministros (PCM), emitirá las directivas necesarias para la ejecución de la presente Ley, en un plazo no mayor de noventa (90) días calendario.

**SEGUNDA.** El Ministerio de Educación (Minedu), adoptara las acciones que correspondan, a efectos de que se incorpore contenidos de ciberseguridad en el currículo escolar.

**TERCERA.** La Autoridad Nacional del Servicio Civil (Servir) y, la Escuela Nacional de Administración Pública (ENAP), incluirán un módulo obligatorio de ciberseguridad en su formación continua para servidores públicos.

**CUARTA.** El Ministerio de Economía y Finanzas (MEF), adoptará las acciones que correspondan, a efectos de que se promueva certificaciones nacionales bajo estándares ISO 27001 y NIST CSF en instituciones críticas del Estado.

Lima, diciembre de 2025

FIRMA DIGITAL
Firmado digitalmente por: PARIONA SINCHE Alfredo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 14:48:13-0500

---

**ALFREDO PARIONA SINCHE**
Congresista de la República

FIRMA DIGITAL
Firmado digitalmente por: DAVILA ATANACIO Pasion Neomias FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 15:03:18-0500

FIRMA DIGITAL
Firmado digitalmente por: QUITO SARMIENTO Bernardo Jaime FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 15:49:34-0500

FIRMA DIGITAL
Firmado digitalmente por: ROBLES ARAUJO Silvana Emperatriz FAU 20161749126 s
Motivo: Soy el autor del documento
Fecha: 01/12/2025 16:35:18-0500

FIRMA DIGITAL
Firmado digitalmente por: FLORES RAMIREZ Alex Randu FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 16:58:59-0500

FIRMA DIGITAL
Firmado digitalmente por: DAVILA ATANACIO Pasion Neomias FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 15:02:58-0500

## EXPOSICIÓN DE MOTIVOS

### FUNDAMENTACIÓN DE LA PROPUESTA:

El numeral 6 del artículo 2 de la Constitución Política del Perú, establece que, *"Toda persona tiene derecho: […] 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar […]".*

Además, el artículo 14-A de la Constitución Política del Perú, señala que, *"El Estado garantiza, a través de la inversión pública o privada, el acceso a internet libre en todo el territorio nacional, con especial énfasis en las zonas rurales, comunidades campesinas y nativas."*

El artículo 16 de la Ley 29733, Ley de protección de datos personales, indica que, *"Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes. Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo."*

Además, el artículo 17 de la Ley 29733, Ley de protección de datos personales, señala que, *"El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales. El obligado puede ser relevado de la obligación de*

*confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional."*

El artículo 2 de la Ley 30096, Ley de Delitos Informáticos, establece que, *"El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."*

De igual modo, el artículo 8 de la Ley 30096, Ley de Delitos Informáticos, señala que, *"El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos."*

El artículo 1 de la Ley 30999, Ley de Ciberdefensa, dispone que, *"La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el*

*ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley."*

El artículo 3 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, establece las siguientes definiciones, *"[…] g) Riesgo de seguridad digital.- Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan. h) Ciberseguridad.- Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país […]".*

Además, el artículo 7 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, indica que, *"7.1 Créase el Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. Asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos. 7.2 El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del*

*Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza. 7.3 El Centro Nacional de Seguridad Digital constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano, de conformidad con el artículo 32 del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. 7.4 El Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional responsable de: i) Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional y, ii) Coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital 7.5 La Secretaría de Gobierno Digital establece los protocolos de escalamiento, coordinación, intercambio y activación ante incidentes de seguridad digital en el país y emite los lineamientos y las directivas correspondientes."*

"La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, es responsable del gobierno, gestión, promoción e impulso, para dictar políticas y estrategias en materia de transformación digital para el uso y aprovechamiento de la Red Nacional del Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE), para lo cual dicta las normas para su adecuado funcionamiento y coordina su implementación con las entidades correspondientes."[1]

"El Ministerio de Transportes y Comunicaciones, a través del Programa Nacional de Telecomunicaciones - PRONATEL, es el responsable de implementar, mantener, operar y supervisar la infraestructura de la Red Nacional del Estado Peruano (REDNACE), así como de desplegar la infraestructura de última milla

[1] Decreto de Urgencia 007-2020. Tercera Disposición Complementaria Final.
LINK: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1252588

para instituciones públicas, para dicho fin, el Ministerio de Transportes y Comunicaciones, dicta normas y coordina su operación con las entidades correspondientes, de conformidad con lo establecido en la Ley Nº 29904, Ley de Promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica y su reglamento."[2]

"La norma ISO/IEC 27001 es el estándar internacional para sistemas de gestión de seguridad de la información (SGSI) de mejores prácticas. Es una especificación rigurosa y completa para proteger y preservar su información bajo los principios de confidencialidad, integridad y disponibilidad. La Norma ofrece un conjunto de controles de mejores prácticas que pueden aplicarse a su organización en función de los riesgos que enfrenta e implementarse de manera estructurada para lograr un cumplimiento certificado y evaluado externamente. El estándar también se puede ampliar integrándolo con varios otros estándares y marcos, incluidos NIST CSF (Marco de ciberseguridad) y NIST RMF (Marco de gestión de riesgos)."[3]

"El 30 de noviembre se celebra en todo el mundo el "Día de la Ciberseguridad" con el objetivo de concienciar sobre los riesgos que se esconden en la red y la importancia de proteger la información digital en un contexto en el que el ciberdelito aumenta año a año y es cada vez más sofisticado. La fecha se instauró en 1988 por iniciativa de la Association for Computing Machinery (ACM), cuando se detectó el primer caso de malware (software malicioso) de propagación en red del mundo."[4]

---

[2] Decreto de Urgencia 007-2020. Tercera Disposición Complementaria Final.
LINK: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1252588

[3] ISO 27001 y el NIST CSF (Marco de Ciberseguridad)
LINK: https://www-itgovernanceusa-com.translate.goog/iso27001-and-nist?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

[4] Santander. 30 de noviembre: Día Mundial de la ciberseguridad. 30 de noviembre de 2022.
LINK: https://www.santanderconsumer.es/simplefinance/blog/tu-futuro/ciberseguridad/post/30-de-noviembre-dia-mundial-de-la-ciberseguridad

"El 3 y 4 de diciembre, se celebra la "Cumbre de ciberamenazas SANS 2025", en el que se reúne la comunidad europea de ciberseguridad. Diseñado para profesionales de la seguridad, este evento abarca disciplinas tanto ofensivas como defensivas, con un enfoque especial en los aspectos técnicos. Ofrece un valor excepcional a profesionales de la ciberseguridad de todos los niveles, ofreciendo un entorno donde pueden compartir experiencias, conocimientos, herramientas y técnicas para impulsar el progreso en este campo. CyberThreat tiene como objetivo ofrecer la mejor conferencia técnica de Europa para profesionales de la ciberseguridad."[5]

Además, según la ONU, "el 3 de diciembre se celebra el Día Internacional de las Personas con Discapacidad, por el que, se planteó la Estrategia de las Naciones Unidas para la Inclusión de la Discapacidad, acorde con su compromiso de hacer que las Naciones Unidas sean una organización inclusiva para todos, la cual constituye la base de un progreso sostenible y transformador hacia la inclusión de la discapacidad en todos los pilares de la labor de la ONU."[6] Lo cual refuerza el principio de accesibilidad y seguridad digital inclusiva, toda vez que, la ciberseguridad no solo protege sistemas, sino también a las personas más vulnerables en el entorno digital.

De igual forma, teniendo coherencia con el ecosistema internacional de derechos digitales, diciembre también es un mes simbólico en materia de derechos digitales, pues el 10 de diciembre se celebra el Día Internacional de los Derechos Humanos, cuyo principio de protección de la privacidad digital se encuentra directamente vinculado con la ciberseguridad.

---

[5] SANS. Cumbre de ciberamenazas SANS 2025.
LINK: https://www.sans.org/cyber-security-training-events/cyberthreat-2025

[6] ONU. Día Internacional de las Personas con Discapacidad 3 de diciembre.
LINK: https://www.un.org/es/observances/day-of-persons-with-disabilities

En la era digital, la ciberseguridad se ha convertido en un componente esencial de la soberanía nacional, la protección de los derechos fundamentales y la estabilidad económica. El Perú, al igual que el resto del mundo, enfrenta crecientes desafíos derivados del cibercrimen, el espionaje digital y la desinformación automatizada. Según el CERT-PERÚ (2024), se registraron más de 22,000 incidentes cibernéticos, afectando tanto a instituciones públicas como privadas. Además, ASBANC estima pérdidas anuales superiores a S/ 3,800 millones por fraudes digitales, y el 60% de usuarios peruanos aún no utiliza autenticación en dos pasos. Estas cifras reflejan una urgente necesidad de concientizar y educar a la población en prácticas seguras en línea.

En tal sentido, en atención a la convergencia internacional, se propone el 3 de diciembre, en armonía con los marcos de cooperación iberoamericana e internacional en materia de ciberseguridad, impulsados por organismos como la SEGIB, la OEI, la UIT y la OEA, pues durante este periodo (noviembre–diciembre) se desarrollan anualmente actividades, informes y foros regionales sobre seguridad digital, que permiten al Perú sincronizar sus esfuerzos de política pública con las tendencias globales y promover la integración regional en materia de confianza digital y soberanía tecnológica.

## EFECTOS DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La vigencia de la presente Ley no contraviene ninguna normativa y se encuentra acorde de los artículos 2, 14-A y, numeral 1 del artículo 102 de la Constitución Política del Perú, puesto que, se propone se declare el día 3 de diciembre de cada año, como el "Día Nacional de la Ciberseguridad", con el propósito de promover la protección de los datos personales, la integridad de las infraestructuras digitales y, la confianza en el uso de las tecnologías de la información y la comunicación (TIC).

## ANÁLISIS COSTO-BENEFICIO

La presente iniciativa legislativa no irroga gasto adicional al erario nacional, puesto que, es una propuesta declarativa que pretende que el día 3 de diciembre de cada año, como el "Día Nacional de la Ciberseguridad", a fin de concientizar, fortalecer las capacidades técnicas y educativas, fomentar la cooperación público-privada y, fomentar la investigación y la innovación en materia de ciberseguridad.

Además, cabe precisar que, diciembre marca el cierre del año académico y presupuestal, lo que facilita la evaluación de políticas públicas en materia de transformación digital y permite proyectar planes de ciber formación para el siguiente año escolar y fiscal. Así, el "Día Nacional de la Ciberseguridad" se convierte en un espacio de balance, reflexión y planificación nacional, por lo que, resulta muy beneficioso para promover una cultura preventiva digital entre ciudadanos, empresas y el Estado, incluso conllevará a fortalecer las capacidades técnicas y la conciencia pública sobre los riesgos cibernéticos; y, establecer un espacio institucional para la coordinación intersectorial en materia de ciberseguridad.

## RELACIÓN CON LAS POLITICAS DE ESTADO EXPRESADAS EN EL ACUERDO NACIONAL

El Proyecto de Ley tiene vinculación directa con la **Novena Política de Estado del Acuerdo Nacional**: "Política de seguridad nacional", en la cual se establece que, nos comprometemos a mantener una política de seguridad nacional que garantice la independencia, soberanía, integridad territorial y la salvaguarda de los intereses nacionales. Consideramos que ésta es una tarea que involucra a la sociedad en su conjunto, a los organismos de conducción del Estado, en especial a las Fuerzas Armadas, en el marco de la Constitución y las leyes. En tal sentido, nos comprometemos a prevenir y afrontar cualquier amenaza externa o interna que ponga en peligro la paz social, la seguridad integral y el bienestar general. […]"

Además, guarda relación con la **Vigésimo Política de Estado del Acuerdo Nacional:** "Desarrollo de la ciencia y la tecnología", en la cual se establece que, nos comprometemos a fortalecer la capacidad del país para generar y utilizar conocimientos científicos y tecnológicos, para desarrollar los recursos humanos y para mejorar la gestión de los recursos naturales y la competitividad de las empresas. De igual manera, nos comprometemos a incrementar las actividades de investigación y el control de los resultados obtenidos, evaluándolos debida y puntualmente. Nos comprometemos también a asignar mayores recursos financieros mediante concursos públicos de méritos que conduzcan a la selección de los mejores investigadores y proyectos, así como a proteger la propiedad intelectual […]"

Lima, diciembre de 2025