

Ley Marco de Ciberseguridad que fortalece el Centro Nacional de Seguridad Digital y organiza el Sistema Nacional de Equipos de Respuesta ante Incidentes de Seguridad Digital

Eleva a rango de ley y dota de potestad supervisora y sancionadora a la autoridad de ciberseguridad civil existente (PCM, a través de la Secretaría de Gobierno y Transformación Digital y el Centro Nacional de Seguridad Digital), sin crear organismo ni pliego; organiza el Sistema Nacional de CSIRT, tipifica infracciones con autoridad competente y deslinda la supervisión de los reguladores sectoriales y la ciberdefensa.

Comisión (Cámara de Diputados): Ciencia, Innovación Tecnológica y Sociedad Digital (+ Modernización de la Gestión del Estado y Contraloría) · **Revisora (Senado):** En asuntos de Salud, Educación, Cultura, Mujer y Desarrollo Social y Digital · **Prioridad:** alta · **Costo fiscal:** bajo · **Plazo:** mediano

Plan Perú 2050: Ciber Seguridad, Perú en La Era Digital, Institucionalidad

I. Exposición de motivos

El Perú no cuenta con una ley general de ciberseguridad. La materia descansa en el Decreto de Urgencia 007-2020 (Marco de Confianza Digital), que crea el Centro Nacional de Seguridad Digital como «plataforma digital» a cargo de la Presidencia del Consejo de Ministros (art. 7) y el Registro Nacional de Incidentes (art. 8), y en su reglamento, el Decreto Supremo 126-2025-PCM, vigente desde febrero de 2026. Ese marco obliga a notificar incidentes solo a los sujetos del numeral 9.1 del artículo 9 del decreto de urgencia (entidades públicas y proveedores de servicios digitales de finanzas, servicios básicos, salud, transporte, internet, actividades críticas y educación); para el resto de organizaciones privadas sus normas son referenciales (numeral 9.2), y no existe un régimen de infracciones y sanciones con rango de ley que permita exigir su cumplimiento. La Ley 30999 solo cubre la ciberdefensa y los reguladores sectoriales (por ejemplo, la SBS con la Resolución SBS 504-2021) aplican estándares propios sin regla de prelación. Según información del Ministerio Público difundida por El Peruano (2-9-2026), se registraron 29 118 denuncias por delitos informáticos entre enero y julio de 2026. En el periodo 2021-2026 se presentaron iniciativas parciales que no llegaron a ser ley. Sin habilitación legal expresa de la potestad sancionadora, las obligaciones de seguridad digital no son verificables ni exigibles.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY MARCO DE CIBERSEGURIDAD QUE FORTALECE EL CENTRO NACIONAL DE SEGURIDAD DIGITAL Y ORGANIZA EL SISTEMA NACIONAL DE EQUIPOS DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DIGITAL

Artículo 1. Objeto

La presente ley tiene por objeto establecer el marco normativo, los principios, las obligaciones y el régimen de supervisión y sanción de la ciberseguridad en el ámbito civil, a fin de proteger la continuidad de los servicios digitales, los derechos de las personas y la confianza digital, en concordancia con el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, y con el Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

Artículo 2. Ámbito de aplicación

2.1. La presente ley se aplica a:

- Las entidades de la administración pública comprendidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado por el Decreto Supremo 006-2026-JUS.
- Los proveedores de servicios digitales comprendidos en el numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020.
- Los operadores de activos críticos nacionales identificados conforme al Decreto Supremo 106-2017-PCM o la norma que lo sustituya.

2.2. Los organismos constitucionalmente autónomos, el Poder Judicial y los gobiernos regionales y locales

aplican las normas técnicas de la Autoridad Nacional de Ciberseguridad en ejercicio de su autonomía, notifican sus incidentes al Centro Nacional de Seguridad Digital y verifican su cumplimiento a través de sus órganos de control institucional.

2.3. La presente ley no comprende las operaciones militares en y mediante el ciberespacio reguladas por la Ley 30999, Ley de Ciberdefensa, ni las actividades del Sistema de Inteligencia Nacional.

Artículo 3. Principios

La aplicación de la presente ley se rige por los principios de seguridad desde el diseño, proporcionalidad según el riesgo, cooperación público-privada, respeto de los derechos fundamentales y de la privacidad, neutralidad tecnológica, mínima intervención en las comunicaciones, transparencia y rendición de cuentas.

Artículo 4. Autoridad Nacional de Ciberseguridad

4.1. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, en su calidad de ente rector de la seguridad digital, es la Autoridad Nacional de Ciberseguridad en el ámbito civil. Ejerce sus funciones operativas a través del Centro Nacional de Seguridad Digital, que actúa con autonomía técnica y funcional.

4.2. La Autoridad Nacional de Ciberseguridad no constituye pliego presupuestal y se financia con cargo al presupuesto institucional de la Presidencia del Consejo de Ministros.

Artículo 5. Funciones de la Autoridad Nacional de Ciberseguridad

Son funciones de la Autoridad Nacional de Ciberseguridad:

- a) Aprobar normas técnicas de ciberseguridad, que constituyen el estándar mínimo para los sujetos del numeral 2.1 del artículo 2.
- b) Supervisar y fiscalizar su cumplimiento y ejercer la potestad sancionadora conforme a los artículos 10 y 11.
- c) Conducir el Equipo de Respuesta a Incidentes de Seguridad Digital Nacional (CSIRT Nacional) y administrar el Registro Nacional de Incidentes de Seguridad Digital.
- d) Emitir alertas y directivas técnicas de mitigación, con los límites del artículo 8.
- e) Aprobar los esquemas de evaluación de la conformidad y reconocer a los evaluadores acreditados por el organismo nacional de acreditación.
- f) Actuar como coordinador nacional de la divulgación coordinada de vulnerabilidades y mantener el canal correspondiente.
- g) Coordinar con el Ministerio de Defensa y el Comando Conjunto de las Fuerzas Armadas el escalamiento de incidentes conforme al artículo 9.
- h) Derivar al Ministerio Público y a la Policía Nacional del Perú los incidentes con indicios de delito, y a la Autoridad Nacional de Protección de Datos Personales los que comprometan datos personales.
- i) Coordinar con el Ministerio de Relaciones Exteriores la cooperación internacional en ciberseguridad civil.

Artículo 6. Sistema Nacional de CSIRT y prelación con los reguladores sectoriales

6.1. El Sistema Nacional de CSIRT está integrado por el CSIRT Nacional, los CSIRT sectoriales que constituyan o designen los organismos reguladores y supervisores, los CSIRT institucionales de las entidades públicas y los CSIRT regionales que se constituyan por convenio con los gobiernos regionales. Los organismos del sistema electoral pueden constituir un CSIRT sectorial integrado al Sistema.

6.2. La Superintendencia de Banca, Seguros y AFP, el Banco Central de Reserva del Perú y los organismos reguladores pueden establecer exigencias de ciberseguridad mayores para sus supervisados; su cumplimiento se presume conforme con las normas técnicas de la Autoridad Nacional de Ciberseguridad.

6.3. La Autoridad Nacional de Ciberseguridad aprueba los protocolos de intercambio de información, clasificación de incidentes y respuesta coordinada.

Artículo 7. Confidencialidad de la información de incidentes

7.1. La información sobre incidentes, vulnerabilidades, indicadores de compromiso y medidas de seguridad recibida o generada por la Autoridad Nacional de Ciberseguridad y por los integrantes del Sistema Nacional de CSIRT constituye información confidencial, conforme al numeral 6 del artículo 17 del Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

7.2. Dicha información solo se divulga en forma agregada y anonimizada, o para alertar a terceros potencialmente afectados sin identificar al notificante. Su entrega al Ministerio Público o al Poder Judicial se

rige por las normas procesales.

7.3. La información notificada no puede ser utilizada como única prueba para imponer sanciones al notificante por los hechos que dieron lugar al incidente.

Artículo 8. Límites de las directivas de mitigación

Las directivas de mitigación son de carácter técnico, temporales, proporcionales, motivadas e impugnables. En ningún caso pueden ordenar el acceso al contenido de comunicaciones privadas, la interceptación o el bloqueo de contenidos por razones distintas de la contención de una amenaza técnica identificada, ni el debilitamiento, la eliminación o la elusión de mecanismos de cifrado. El acceso al contenido de las comunicaciones requiere mandato judicial conforme al numeral 10 del artículo 2 de la Constitución Política del Perú.

Artículo 9. Escalamiento a ciberdefensa

La Autoridad Nacional de Ciberseguridad y el Ministerio de Defensa aprueban, mediante decreto supremo refrendado por el Presidente del Consejo de Ministros y el Ministro de Defensa, el protocolo de escalamiento de incidentes que afecten la seguridad nacional o los activos críticos nacionales, conforme a la Ley 30999 y su reglamento aprobado por el Decreto Supremo 017-2024-PCM. El protocolo define umbrales, roles y la conducción civil de la respuesta en los demás casos.

Artículo 10. Infracciones

10.1. Las infracciones se clasifican en leves, graves y muy graves.

10.2. Son infracciones leves: a) no designar al responsable de seguridad digital cuando sea exigible; b) no actualizar la información de contacto ante el CSIRT Nacional; c) presentar fuera de plazo los informes periódicos de ciberseguridad exigidos por las normas técnicas.

10.3. Son infracciones graves: a) no notificar un incidente de seguridad digital significativo dentro del plazo legal; b) no implementar las medidas mínimas de gestión de riesgos de seguridad digital establecidas en las normas técnicas; c) no cumplir una directiva de mitigación ordinaria dentro del plazo fijado; d) reincidir en una infracción leve dentro de un año.

10.4. Son infracciones muy graves: a) incumplir una directiva de mitigación emitida ante un incidente en curso que afecte la continuidad de un servicio esencial; b) ocultar o falsear información sobre un incidente; c) obstruir o impedir la supervisión; d) reincidir en una infracción grave dentro de un año.

10.5. Conforme al numeral 4 del artículo 248 del Texto Único Ordenado de la Ley 27444, el reglamento puede especificar o graduar las conductas descritas en los numerales precedentes, sin crear infracciones nuevas.

Artículo 11. Sanciones y autoridad competente

11.1. Las infracciones leves se sancionan con amonestación o multa de hasta cincuenta unidades impositivas tributarias; las graves, con multa de más de cincuenta hasta trescientas unidades impositivas tributarias; y las muy graves, con multa de más de trescientas hasta mil unidades impositivas tributarias. La multa no excede el diez por ciento de los ingresos brutos anuales del infractor del ejercicio anterior y se gradúa conforme al numeral 3 del artículo 248 del Texto Único Ordenado de la Ley 27444, considerando además el tamaño del infractor.

11.2. Cuando el infractor esté sujeto a la supervisión de un organismo regulador o supervisor sectorial, la potestad sancionadora corresponde a este, aplicando la presente ley; la Autoridad Nacional de Ciberseguridad ejerce la potestad sancionadora respecto de los sujetos privados que no cuenten con supervisor sectorial. En ningún caso se sanciona dos veces el mismo hecho con identidad de sujeto y fundamento.

11.3. Las entidades públicas no son sancionadas con multa. El incumplimiento de la presente ley por servidores y funcionarios públicos constituye falta disciplinaria conforme a la Ley 30057, Ley del Servicio Civil, sin perjuicio de la responsabilidad administrativa funcional que determine la Contraloría General de la República conforme a la Ley 27785.

11.4. El producto de las multas impuestas por la Autoridad Nacional de Ciberseguridad constituye recurso de la Presidencia del Consejo de Ministros y no financia gasto permanente.

Artículo 12. Consejo Consultivo de Ciberseguridad

La Autoridad Nacional de Ciberseguridad conforma un Consejo Consultivo de Ciberseguridad, de carácter ad honorem, integrado por representantes de la academia, gremios empresariales, colegios profesionales, sociedad civil y comunidad técnica, que emite opinión no vinculante sobre la Estrategia Nacional de

Ciberseguridad y los proyectos de normas técnicas. Su funcionamiento no irroga gasto al Estado.

Artículo 13. Estrategia Nacional de Ciberseguridad

La Autoridad Nacional de Ciberseguridad formula la Estrategia Nacional de Ciberseguridad con horizonte quinquenal, articulada a la Política Nacional de Transformación Digital, que se aprueba por decreto supremo con el voto aprobatorio del Consejo de Ministros y se evalúa anualmente mediante un informe público de indicadores.

Primera. Disposición Complementaria Final

Reglamentación. El Poder Ejecutivo, mediante decreto supremo refrendado por el Presidente del Consejo de Ministros, reglamenta la presente ley en un plazo no mayor de ciento veinte días hábiles contados a partir del día siguiente de su publicación, y adecúa el Decreto Supremo 126-2025-PCM.

Segunda. Disposición Complementaria Final

Financiamiento. La implementación de la presente ley se financia con cargo al presupuesto institucional de la Presidencia del Consejo de Ministros, sin demandar recursos adicionales al Tesoro Público. Cualquier fortalecimiento que requiera recursos adicionales se sujeta a la programación multianual y a la disponibilidad presupuestal, previo informe del Ministerio de Economía y Finanzas.

Tercera. Disposición Complementaria Final

Evaluación de un organismo técnico especializado. Se encarga al Poder Ejecutivo evaluar, en un plazo de doce meses contados a partir de la entrada en vigencia del reglamento, la conveniencia de constituir un organismo técnico especializado en ciberseguridad conforme a los artículos 28 y 29 de la Ley 29158, Ley Orgánica del Poder Ejecutivo, y, de ser el caso, proponer la iniciativa legislativa correspondiente.

Cuarta. Disposición Complementaria Final

Funciones vinculadas a la inteligencia artificial. Lo dispuesto en la presente ley no afecta las funciones de monitoreo de sistemas de inteligencia artificial que el Reglamento de la Ley 31814, aprobado por el Decreto Supremo 115-2025-PCM, asigna al órgano de la Secretaría de Gobierno y Transformación Digital que administra el Centro Nacional de Seguridad Digital.

Única. Disposición Complementaria Transitoria

Gradualidad sancionadora. Durante los dieciocho meses siguientes a la entrada en vigencia del reglamento, la Autoridad Nacional de Ciberseguridad y los supervisores sectoriales priorizan acciones de orientación y subsanación respecto de los sujetos privados; la potestad sancionadora respecto de ellos se ejerce a partir del día siguiente de vencido dicho plazo.

Primera. Disposición Complementaria Modificatoria

Modificación del artículo 7 del Decreto de Urgencia 007-2020. Se modifica 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, en los términos siguientes:

«Artículo 7. Centro Nacional de Seguridad Digital

7.1. El Centro Nacional de Seguridad Digital 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. Es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional.

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 y Transformación Digital, actúa con autonomía técnica y funcional y es el único punto de contacto nacional con 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, conforme al artículo 32 del Decreto Legislativo 1412.

7.4. El Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional, responsable de gestionar la respuesta y recuperación ante incidentes de seguridad digital en

el ámbito nacional y de coordinar con equipos de similar naturaleza nacionales e internacionales.

7.5. La Secretaría de Gobierno y Transformación Digital, en su calidad de Autoridad Nacional de Ciberseguridad, ejerce las funciones de supervisión, fiscalización y sanción previstas en la Ley Marco de Ciberseguridad, y aprueba los protocolos de escalamiento, coordinación, intercambio y activación ante incidentes de seguridad digital.»

Segunda. Disposición Complementaria Modificatoria

Modificación del numeral 9.2 del artículo 9 del Decreto de Urgencia 007-2020. Se modifica el numeral 9.2 del artículo 9 del Decreto de Urgencia 007-2020, en los términos siguientes:

«Artículo 9. Obligaciones del Proveedor de servicios digitales

[...]

9.2. Las organizaciones privadas no comprendidas en el numeral 9.1 ni en el ámbito de la Ley Marco de Ciberseguridad toman como referencia las normas emitidas por la Secretaría de Gobierno y Transformación Digital en cuanto les aplique y les genere valor, e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.»

III. Análisis costo-beneficio

La propuesta no crea organismo ni pliego: fortalece una estructura existente (Secretaría de Gobierno y Transformación Digital y Centro Nacional de Seguridad Digital) y se financia con su presupuesto institucional, sin demandar recursos adicionales al Tesoro Público. Su principal costo incremental es la función de supervisión y sanción, estimado por el editor en S/ 3 a 6 millones anuales si se implementa plenamente (supuestos en la ficha de impacto); por el criterio de la STC 00018-2023-PI/TC, cualquier fortalecimiento que requiera recursos adicionales queda sujeto a la programación multianual y a informe previo del MEF. El beneficio principal es convertir guías referenciales en obligaciones exigibles con un régimen sancionador tipificado, una regla clara de prelación con los reguladores (que evita la doble sanción) y garantías de confidencialidad que incentivan el reporte de incidentes. La gradualidad de dieciocho meses y el tope del diez por ciento de los ingresos protegen a las mipymes.

Normas que modifica

- Decreto de Urgencia 007-2020, Marco de Confianza Digital, art. 7 — *modifica*
- Decreto de Urgencia 007-2020, Marco de Confianza Digital, art. 9, num. 9.2 — *modifica*
- Decreto Legislativo 1412, Ley de Gobierno Digital, arts. 30 a 33 (Marco de Seguridad Digital) — *complementa*
- Ley 30999, Ley de Ciberdefensa, deslinde de ámbito — *complementa*
- Decreto Supremo 126-2025-PCM, Reglamento del D.U. 007-2020, adecuación integral — *complementa*

Entidades implicadas (quién hace qué)

- **PCM-SGTD** (rectora): Ejerce como Autoridad Nacional de Ciberseguridad: aprueba normas técnicas, supervisa y sanciona a privados sin supervisor sectorial (arts. 4, 5, 10 y 11); formula la Estrategia Nacional (art. 13).
- **CNSD** (ejecutora): Conduce el CSIRT Nacional, administra el Registro Nacional de Incidentes, emite alertas y coordina la divulgación de vulnerabilidades (art. 5, literales c, d y f; DCM Primera).
- **SBS / reguladores** (sancionadora): Supervisan y sancionan a sus regulados aplicando la ley y pueden fijar exigencias mayores; constituyen CSIRT sectoriales (arts. 6.1, 6.2 y 11.2).
- **MINDEF / CCFFAA** (consultiva): Aprueba con la PCM el protocolo de escalamiento a ciberdefensa (art. 9).
- **MP / PNP** (beneficiaria): Reciben la derivación de incidentes con indicios de delito (art. 5, literal h).
- **ANPD** (supervisora): Recibe incidentes que comprometen datos personales (art. 5, literal h).
- **MEF** (financiadora): Emite informe previo ante cualquier requerimiento de recursos adicionales (DCF Segunda).
- **CGR / SERVIR** (supervisora): Responsabilidad funcional y régimen disciplinario de servidores por incumplimiento (art. 11.3).

Sujetos obligados: Entidades de la administración pública (art. I del TUO de la Ley 27444); proveedores de servicios digitales del numeral 9.1 del artículo 9 del D.U. 007-2020 (finanzas, energía, agua, gas, salud, transporte de personas, internet, actividades críticas y educación); operadores de activos críticos nacionales.

Beneficiarios: Usuarios de servicios digitales públicos y privados en todo el país; entidades públicas y empresas que reciben alertas y apoyo del CSIRT Nacional. No se cuantifica el número de beneficiarios por falta de una cifra oficial agregada.

Impacto económico estimado (confianza baja; referencial, no oficial)

Tipo: gasto

Costo para el Estado: S/ 3–6 millones/año (estimación del editor)

Horizonte: anual, desde 2028

Financiamiento: Presupuesto institucional de la PCM sin demandar recursos adicionales al Tesoro Público. El fortalecimiento por encima de ese marco requiere coordinación con el Poder Ejecutivo, fuente de financiamiento identificada e informe previo de sostenibilidad fiscal del MEF antes del dictamen (STC 00018-2023-PI/TC).

Supuestos: Unidad de supervisión y sanción y refuerzo del CSIRT Nacional con 15 a 25 especialistas (sin crear pliego), con costo laboral anual de S/ 170 000 a S/ 210 000 por plaza (remuneración mensual de S/ 12 000 a S/ 15 000 por 14 pagos, supuesto propio sin fuente oficial), más S/ 0,5 a 1 millón anual en herramientas. No incluye el costo de adecuación de las entidades públicas, que ya están obligadas por el art. 9.3 del D.U. 007-2020.

Beneficio para el Estado: Reducción del riesgo de interrupción de servicios públicos digitales y de los costos de recuperación ante incidentes; recaudación por multas (incierto, no se usa para financiar gasto permanente). No cuantificable con información pública.

Beneficio para la sociedad: Mayor continuidad de servicios esenciales, reporte de incidentes con garantías de confidencialidad y reglas claras que evitan doble supervisión. No cuantificable con información pública.

Inversión privada: Inversión de los sujetos obligados en controles de seguridad y servicios de evaluación de conformidad; no cuantificable con información pública.

Costo para privados: Costos de cumplimiento para los proveedores del art. 9.1 del D.U. 007-2020 (ya obligados a notificar y gestionar riesgos), acotados por la gradualidad de 18 meses y el tope del 10 % de ingresos en las multas.

Riesgos: Insuficiencia de personal especializado por escalas remunerativas públicas; resistencia de reguladores a la prelación; que la confidencialidad se use para ocultar incidentes de interés público (mitigado con reportes agregados).

Revisión especializada (asistida por IA, sobre la versión anterior)

- **Constitucional** — Observaciones graves: La necesidad de una autoridad de ciberseguridad con potestad sancionadora es legítima, pero crear la Agencia como organismo técnico especializado con pliego propio choca con el art. 28 de la LOPE (creación por ley a iniciativa del Ejecutivo) y con la prohibición de iniciativa parlamentaria de gasto (art. 79; STC 00018-2023-PI/TC). Además, la tipificación de infracciones es una norma en blanco y no se resuelve la concurrencia con la SBS ni la sujeción de los organismos autónomos.
- **Técnica legislativa** — Observaciones graves: Una ley marco de ciberseguridad es necesaria y la propuesta deslinda bien el ámbito frente a la ciberdefensa. Sin embargo, crea un organismo técnico especializado y un pliego, lo que es iniciativa del Poder Ejecutivo y genera gasto (art. 28 de la Ley 29158 y art. 79 de la Constitución). Su régimen sancionador es una norma en blanco con multa única de hasta mil UIT, superpone la rectoría con la Secretaría de Gobierno y Transformación Digital sin modificar el Decreto Legislativo 1412 y remite a una «ley de la materia» inexistente.
- **Concordancia normativa** — Observaciones graves: Diagnóstico y normas citadas verificados (D.U. 007-2020; D.S. 126-2025-PCM, publicado nov-2025 y vigente a los 90 días; Ley 30999; Res. SBS 504-2021). Pero crea un organismo técnico especializado por iniciativa congresal contra el art. 28 de la Ley 29158, su modificatoria del D.U. 007-2020 es genérica y su régimen sancionador colisiona con CIB-02 (supervisión sectorial), generando riesgo de doble sanción.
- **Seguridad** — Con observaciones: Pieza central y técnicamente bien orientada: deslinda ciberseguridad civil de ciberdefensa, crea un CSIRT nacional con red sectorial y potestad sancionadora gradual. Faltan garantías jurídicas para el intercambio de información de incidentes (confidencialidad frente a la Ley 27806 y no autoincriminación), límites expresos a las directivas de mitigación para evitar intervenciones en comunicaciones o bloqueos de contenido, y un protocolo de escalamiento a ciberdefensa con umbrales definidos.

• **Derecho tecnológico** — Observaciones graves: El diagnóstico es correcto: el DU 007-2020 y el DS 126-2025-PCM (vigente desde febrero de 2026) carecen de régimen sancionador, y la notificación obligatoria al CNSD solo alcanza a los sujetos del art. 9.1 del DU. Sin embargo, la creación de un OTE por iniciativa no gubernamental choca con el art. 28 de la Ley 29158 y con el art. 79 de la Constitución. Además, separar la ciberseguridad de la SGTD fragmenta la rectoría del DL 1412 y deja sin soporte el monitoreo de IA que el DS 115-2025-PCM (art. 35) encarga al CNSD.

IV. Efecto de la vigencia de la norma

Modifica el artículo 7 y el numeral 9.2 del artículo 9 del Decreto de Urgencia 007-2020; complementa el Decreto Legislativo 1412 (Marco de Seguridad Digital) sin alterar la rectoría de la Secretaría de Gobierno y Transformación Digital; complementa la Ley 30999 (deslinde con ciberdefensa); declara información confidencial conforme al numeral 6 del artículo 17 del TUO de la Ley 27806; obliga a adecuar el Decreto Supremo 126-2025-PCM. No modifica la Ley 29158: encarga al Poder Ejecutivo evaluar un organismo técnico especializado conforme a sus artículos 28 y 29. No requiere votación de ley orgánica.

V. Indicador de éxito al 2031

A 2031, régimen sancionador reglamentado y aplicado, al menos 10 CSIRT sectoriales y regionales integrados al Sistema Nacional, Estrategia Nacional de Ciberseguridad evaluada anualmente con informe público y evaluación del Poder Ejecutivo sobre el organismo técnico especializado publicada.

Normas relacionadas

- Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento — https://www3.congreso.gob.pe/Docs/comisiones2020/ConstitucionReglamento/files/du_interregno_2020/du-007-2020.pdf
- Decreto Supremo 126-2025-PCM, Reglamento del Decreto de Urgencia 007-2020 (Marco de Confianza Digital) — <https://busquedas.elperuano.pe/dispositivo/EX/2455024-1>
- Decreto Legislativo 1412, Ley de Gobierno Digital — <https://busquedas.elperuano.pe/dispositivo/NL/1691026-1>
- Ley 30999, Ley de Ciberdefensa (2019) — https://www3.congreso.gob.pe/Docs/DGP/DIDP/files/ley_30999.pdf
- Decreto Supremo 017-2024-PCM, Reglamento de la Ley 30999 — https://www3.congreso.gob.pe/Docs/DGP/DIDP/files/ds_017-2024-pcm.pdf
- Decreto Supremo 085-2023-PCM, Política Nacional de Transformación Digital al 2030 — <https://busquedas.elperuano.pe/dispositivo/NL/2200457-5>
- Resolución SBS 504-2021, Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad — <https://busquedas.elperuano.pe/dispositivo/NL/1929393-1>

Antecedentes

Periodo 2021-2026 (según verificación en SPLEY del revisor normativo): PL 09906/2024-CR, Ley de seguridad digital o ciberseguridad (con dictamen); PL 08842/2024-CR, interés nacional del Comité de Alto Nivel de Ciberseguridad (con dictamen); PL 12926/2025-CR, Superintendencia Nacional de Transformación y Seguridad Digital (en comisión); PL 13568/2025-CR, fortalecimiento del sistema nacional de ciberseguridad para infraestructuras críticas (en comisión); PL 01776/2021-CR, Centro Nacional de Ciberseguridad (orden del día). Ninguno fue publicado como ley.

Referencias internacionales

- Chile: Ley 21.663, Ley Marco de Ciberseguridad (crea la Agencia Nacional de Ciberseguridad y CSIRT) — <https://www.bcn.cl/leychile/navegar?idNorma=1202434>
- Unión Europea: Directiva (UE) 2022/2555 (NIS2), medidas para un elevado nivel común de ciberseguridad — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- Singapur: Cybersecurity Act 2018 — <https://sso.agc.gov.sg/Act/CA2018>

- España: Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información — <https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257>

Fuentes

- Decreto de Urgencia 007-2020 (copia del Congreso) — https://www3.congreso.gob.pe/Docs/comisiones2020/ConstitucionReglamento/files/du_interregno_2020/du-007-2020.pdf
- Decreto Supremo 126-2025-PCM (El Peruano) — <https://busquedas.elperuano.pe/dispositivo/EX/2455024-1>
- El Peruano (02-09-2026): Ciberdelitos más denunciados en el Perú — 29 118 denuncias ene-jul 2026 según el Ministerio Público — <https://elperuano.pe/noticia/303867-ciberdelitos-mas-denunciados-en-el-peru>
- Apaxi (07-09-2026): Normas de ciberseguridad para empresas en el Perú — <https://apaxi.info/2026/09/07/normas-ciberseguridad-empresas-peru/>
- Proyecto de Ley 9906/2024-CR, Ley de Seguridad Digital o Ciberseguridad (copia LP Derecho) — https://img.lpderecho.pe/wp-content/uploads/2025/01/Proyecto-de-Ley-9906-2024-CR-LPDerecho_.pdf

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/CIB-01.html>