

Ley que establece el contenido mínimo, la verificación y el régimen sancionador de las obligaciones de ciberseguridad de los operadores de servicios esenciales

Desarrolla las obligaciones del artículo 9 del Decreto de Urgencia 007-2020 para los operadores de servicios esenciales: fija su contenido mínimo verificable (gestión de riesgos, controles técnicos, continuidad, cadena de suministro, auditoría independiente), habilita expresamente a los reguladores sectoriales para supervisar y sancionar, y tipifica las infracciones en la ley.

Comisión (Cámara de Diputados): Defensa del Consumidor y Regulación de los Servicios Públicos (+ Ciencia, Innovación Tecnológica y Sociedad Digital) · **Revisora (Senado):** Economía, Medio Ambiente y Defensa del Consumidor · **Prioridad:** alta ·

Costo fiscal: bajo · **Plazo:** mediano

Plan Perú 2050: Ciber Seguridad, Defensa, Infraestructura y Construcción

I. Exposición de motivos

La protección de infraestructuras críticas se rige por el Decreto Supremo 106-2017-PCM (Activos Críticos Nacionales, coordinado por la Dirección Nacional de Inteligencia), con enfoque de seguridad y defensa. El numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020 ya obliga a las entidades públicas y a los proveedores de servicios digitales de finanzas, energía eléctrica, agua, gas, salud, transporte de personas, internet, actividades críticas y educación a notificar incidentes, gestionar riesgos e implementar medidas de seguridad, y el Decreto Supremo 126-2025-PCM desarrolla esas obligaciones. El vacío no es la existencia de la obligación sino su contenido mínimo verificable (sistemas de gestión, controles para tecnología operacional, continuidad probada, cadena de suministro, auditoría) y la ausencia de un régimen sancionador: las leyes de OSINERGMIN, SUNASS, OSITRAN, OSIPTEL y SUSALUD no tipifican incumplimientos de ciberseguridad. Solo el sistema financiero cuenta con regulación desarrollada (Resolución SBS 504-2021). Así, un ataque de ransomware puede paralizar un hospital o una empresa de agua sin que exista obligación exigible de contar con planes de continuidad probados ni auditorías. Experiencias como la Directiva NIS2 de la Unión Europea o la SOCI Act australiana muestran que obligaciones proporcionales y verificables son la base de la resiliencia.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE ESTABLECE EL CONTENIDO MÍNIMO, LA VERIFICACIÓN Y EL RÉGIMEN SANCIONADOR DE LAS OBLIGACIONES DE CIBERSEGURIDAD DE LOS OPERADORES DE SERVICIOS ESENCIALES

Artículo 1. Objeto

La presente ley desarrolla, para los operadores de servicios esenciales, las obligaciones del artículo 9 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, estableciendo su contenido mínimo, los mecanismos de verificación y el régimen de infracciones y sanciones, a fin de garantizar la continuidad de los servicios de los que dependen la vida, la salud, la seguridad y la actividad económica de la población.

Artículo 2. Operadores de servicios esenciales

2.1. Son operadores de servicios esenciales las entidades públicas y las personas jurídicas de derecho privado comprendidas en el numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020 que, conforme a los criterios del artículo 3, sean calificadas como tales, así como los operadores de activos críticos nacionales identificados conforme al Decreto Supremo 106-2017-PCM.

2.2. Por ley pueden incorporarse otros sectores. El Poder Ejecutivo, mediante decreto supremo con voto aprobatorio del Consejo de Ministros y previo informe técnico publicado, puede precisar los subsectores comprendidos en los sectores enumerados en el numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020.

Artículo 3. Calificación de operadores

3.1. El organismo regulador o supervisor del sector o, en su defecto, el ministerio rector califica como operador de servicio esencial a quien cumpla al menos uno de los criterios siguientes: número de usuarios atendidos, dependencia de otros sectores respecto de su servicio, impacto territorial de su interrupción y ausencia de alternativas inmediatas. El reglamento fija los umbrales de cada criterio.

3.2. La calificación se notifica al operador y es impugnabile conforme al Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado por el Decreto Supremo 006-2026-JUS.

3.3. El número de operadores calificados por sector es público. El detalle técnico de la lista constituye información reservada por razones de seguridad nacional en los términos del artículo 16 del Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

3.4. Los organismos constitucionalmente autónomos que presten servicios esenciales aplican las obligaciones del artículo 4 en ejercicio de su autonomía y remiten el informe de auditoría al Centro Nacional de Seguridad Digital; no están sujetos a la potestad sancionadora del artículo 8.

Artículo 4. Obligaciones mínimas

Los operadores de servicios esenciales:

- a) Implementan un sistema de gestión de seguridad de la información basado en estándares reconocidos, como la serie NTP-ISO/IEC 27000.
- b) Designan un oficial de seguridad y confianza digital con el perfil previsto en el reglamento del Decreto de Urgencia 007-2020 y con acceso directo a la alta dirección.
- c) Mantienen planes de continuidad y recuperación probados al menos una vez al año.
- d) Gestionan el riesgo de la cadena de suministro tecnológica.
- e) Notifican los incidentes de seguridad digital al Centro Nacional de Seguridad Digital, o al órgano que haga sus veces, y a su supervisor sectorial, conforme al Decreto de Urgencia 007-2020 y su reglamento o la norma que los sustituya.
- f) Aplican las directivas de mitigación que emita la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, o la entidad que asuma sus funciones por ley.
- g) Aplican controles mínimos que comprenden autenticación multifactor para accesos remotos y privilegiados, segmentación entre redes de tecnologías de la información y de tecnología operacional, respaldos protegidos y desconectados con pruebas de restauración, gestión de vulnerabilidades y conservación de registros de eventos por al menos doce meses, conforme a la norma técnica que apruebe la Secretaría de Gobierno y Transformación Digital tomando como referencia la serie NTP-ISO/IEC 27000 y, para sistemas de control industrial, la serie IEC 62443.

Artículo 5. Responsabilidad de la alta dirección

El directorio o máximo órgano de gobierno del operador aprueba la política de ciberseguridad, asigna los recursos necesarios y recibe, al menos semestralmente, un informe sobre el estado del riesgo de seguridad digital. Sus integrantes acreditan capacitación básica en gestión de riesgos de seguridad digital.

Artículo 6. Auditorías

6.1. Los operadores se someten a una auditoría de ciberseguridad cada dos años, realizada por organismos de evaluación de la conformidad acreditados por el Instituto Nacional de Calidad conforme a la Ley 30224, o por organismos de acreditación signatarios de acuerdos de reconocimiento multilateral internacionales. El informe se remite al supervisor sectorial y a la Secretaría de Gobierno y Transformación Digital.

6.2. El auditor no puede auditar a un operador al que haya prestado servicios de implementación de seguridad en los dos años previos.

6.3. El supervisor puede disponer auditorías extraordinarias ante incidentes significativos.

6.4. Para los operadores del régimen simplificado del artículo 9, la auditoría puede ser interna con revisión del supervisor sectorial o de la Secretaría de Gobierno y Transformación Digital.

Artículo 7. Articulación con los Activos Críticos Nacionales

Los operadores que administren activos críticos nacionales conforme al Decreto Supremo 106-2017-PCM integran las obligaciones de la presente ley en sus planes de seguridad. La Secretaría de Gobierno y Transformación Digital y la Dirección Nacional de Inteligencia aprueban un protocolo de intercambio de información reservada.

Artículo 8. Potestad sancionadora

- 8.1. Se atribuye a los organismos reguladores y supervisores sectoriales la potestad de supervisar y sancionar el incumplimiento de la presente ley respecto de los operadores bajo su competencia.
- 8.2. En los sectores sin supervisor sectorial, la potestad corresponde a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, o a la entidad que asuma sus funciones por ley.
- 8.3. Las empresas supervisadas por la Superintendencia de Banca, Seguros y AFP y los administradores de sistemas de pagos y de liquidación de valores supervisados por el Banco Central de Reserva del Perú conforme a la Ley 29440 se rigen por la regulación y la potestad sancionadora de dichas entidades.
- 8.4. En ningún caso se sanciona dos veces el mismo hecho con identidad de sujeto y fundamento.
- 8.5. Respecto de las entidades públicas, el incumplimiento constituye falta disciplinaria de los servidores responsables conforme a la Ley 30057, Ley del Servicio Civil, sin perjuicio de la responsabilidad administrativa funcional.

Artículo 9. Infracciones y sanciones

- 9.1. Son infracciones leves: a) no comunicar al supervisor la designación del oficial de seguridad y confianza digital; b) remitir fuera de plazo el informe de auditoría.
- 9.2. Son infracciones graves: a) no implementar las obligaciones de los literales a), c), d) o g) del artículo 4; b) no someterse a la auditoría del artículo 6; c) reincidir en una infracción leve dentro de un año.
- 9.3. Son infracciones muy graves: a) no notificar un incidente significativo conforme al literal e) del artículo 4; b) incumplir una directiva de mitigación conforme al literal f) del artículo 4; c) falsear el informe de auditoría o la información remitida al supervisor; d) reincidir en una infracción grave dentro de un año.
- 9.4. 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, sin exceder el diez por ciento de los ingresos brutos anuales del infractor del ejercicio anterior.
- 9.5. Conforme al numeral 4 del artículo 248 del Texto Único Ordenado de la Ley 27444, el reglamento puede especificar o graduar las conductas descritas, sin crear infracciones nuevas.

Artículo 10. Proporcionalidad y régimen simplificado

El reglamento establece un régimen simplificado para operadores de menor tamaño, empresas prestadoras de servicios de saneamiento municipales y gobiernos locales, que conserva las obligaciones de los literales b), c) y e) del artículo 4. En este régimen, el oficial de seguridad y confianza digital puede ser compartido entre varias entidades u operadores, o provisto por el gobierno regional mediante convenio.

Primera. Disposición Complementaria Final

Reglamentación. El Poder Ejecutivo, mediante decreto supremo refrendado por el Presidente del Consejo de Ministros y los ministros de los sectores comprendidos, reglamenta la presente ley en un plazo no mayor de ciento veinte días hábiles contados a partir del día siguiente de su publicación.

Segunda. Disposición Complementaria Final

Equivalencia del régimen financiero. Las empresas que cumplan la regulación de la Superintendencia de Banca, Seguros y AFP sobre gestión de la seguridad de la información y ciberseguridad se consideran conformes con el artículo 4, sin perjuicio de las auditorías del artículo 6.

Tercera. Disposición Complementaria Final

Financiamiento. La implementación de la presente ley se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Cuarta. Disposición Complementaria Final

Articulación con la ley marco de ciberseguridad. Si se aprueba una ley que atribuya a otra entidad las funciones de autoridad nacional de ciberseguridad, las referencias de la presente ley a la Secretaría de Gobierno y Transformación Digital se entienden hechas a dicha entidad.

Única. Disposición Complementaria Transitoria

Plazo de adecuación. Los operadores calificados cuentan con dieciocho meses desde la notificación de su calificación para cumplir las obligaciones del artículo 4 y con treinta meses para la primera auditoría. La potestad sancionadora respecto de dichas obligaciones se ejerce a partir del vencimiento de esos plazos.

Única. Disposición Complementaria Modificatoria

Modificación del numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020. Se modifica el numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020, en los términos siguientes:

«Artículo 9. Obligaciones del Proveedor de servicios digitales

9.1. Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, hidrocarburos, agua y gas), salud, transporte de personas, telecomunicaciones, servicios de emergencia, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos deben:

- a) Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
- b) Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.
- c) Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.
- d) Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.
- e) Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.
- f) Mantener una infraestructura segura, escalable e interoperable.

Los proveedores calificados como operadores de servicios esenciales cumplen, además, las obligaciones de la ley de la materia.»

III. Análisis costo-beneficio

El costo recae principalmente en los operadores calificados (sistemas de gestión, controles técnicos, auditorías bienales, personal especializado). Para el Estado, el costo incremental es bajo: la supervisión se encarga a reguladores existentes, financiados mayoritariamente con el aporte por regulación, y a la Secretaría de Gobierno y Transformación Digital en forma residual; el editor lo estima en S/ 2 a 4 millones anuales con supuestos explícitos. Los operadores públicos (hospitales, empresas de agua municipales) enfrentan costos de adecuación que se mitigan con el régimen simplificado, la auditoría interna revisada y el oficial compartido. El beneficio es la reducción de la probabilidad e impacto de interrupciones de servicios vitales; no existe cuantificación oficial en el Perú. La equivalencia con la regulación SBS y la regla de non bis in idem evitan duplicidad. No demanda recursos adicionales al Tesoro Público.

Normas que modifica

- Decreto de Urgencia 007-2020, Marco de Confianza Digital, art. 9, num. 9.1 — *modifica*
- Decreto Supremo 106-2017-PCM, Activos Críticos Nacionales, articulación (art. 7 de la ley) — *complementa*
- Decreto Supremo 126-2025-PCM, Reglamento del D.U. 007-2020, adecuación de obligaciones de proveedores — *complementa*
- Resolución SBS 504-2021, equivalencia (DCF Segunda) — *complementa*

Entidades implicadas (quién hace qué)

- **Reguladores** (sancionadora): Califican operadores (art. 3), supervisan y sancionan con la escala del art. 9 (art. 8.1).
- **PCM-SGTD** (rectora): Aprueba la norma técnica de controles mínimos (art. 4.g), recibe auditorías (art. 6), emite directivas (art. 4.f) y sanciona en sectores sin supervisor (art. 8.2).
- **SBS / BCRP** (supervisora): Mantienen su regulación y potestad sobre entidades financieras y sistemas de pagos (art. 8.3; DCF Segunda).
- **DINI** (consultiva): Protocolo de intercambio de información reservada sobre activos críticos (art. 7).

- **INACAL** (ejecutora): Acredita organismos de evaluación de la conformidad para las auditorías (art. 6.1).
- **Ministerios** (reguladora): Califican operadores en sectores sin regulador (art. 3.1).

Sujetos obligados: Operadores calificados de los sectores del numeral 9.1 del art. 9 del D.U. 007-2020 (finanzas, energía eléctrica, hidrocarburos, agua, gas, salud, transporte de personas, telecomunicaciones, emergencias, internet, actividades críticas, educación) y operadores de activos críticos nacionales; régimen simplificado para operadores pequeños, EPS municipales y gobiernos locales.

Beneficiarios: Usuarios de servicios de energía, agua, salud, transporte, telecomunicaciones y finanzas de todo el país; no se cuantifica por falta de un registro público de operadores.

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

Tipo: gasto

Costo para el Estado: S/ 2–4 millones/año (estimación del editor, supervisión); adecuación de operadores públicos no cuantificable con información pública

Horizonte: anual, desde 2028

Financiamiento: Presupuesto institucional de los reguladores (financiados mayoritariamente con el aporte por regulación) y de la PCM, sin demandar recursos adicionales al Tesoro Público. Si la adecuación de operadores públicos requiere recursos adicionales, se necesita coordinación con el Poder Ejecutivo, fuente de financiamiento identificada e informe previo de sostenibilidad fiscal del MEF antes del dictamen.

Supuestos: Seis supervisores (OSINERGMIN, SUNASS, OSIPTEL, OSITRAN, SUSALUD y SGTD residual) con 2 a 3 especialistas cada uno a un costo laboral anual de S/ 170 000 a S/ 210 000 por plaza (supuesto propio, sin fuente oficial). No incluye la inversión de hospitales públicos y EPS municipales en controles, que depende del número de operadores calificados (desconocido).

Beneficio para el Estado: Menor probabilidad de interrupciones de servicios públicos críticos y de costos de recuperación; recaudación por multas incierta. No cuantificable con información pública.

Beneficio para la sociedad: Continuidad de servicios vitales (agua, energía, salud, pagos) y reglas homogéneas entre sectores. No cuantificable con información pública.

Inversión privada: Demanda de servicios de auditoría, evaluación de conformidad y seguridad de tecnología operacional; no cuantificable con información pública.

Costo para privados: Implementación de SGSI, controles técnicos, pruebas de continuidad y auditoría bienal; según un supuesto del revisor de seguridad, del orden de cientos de miles de soles iniciales y recurrentes para un operador mediano (no verificado). Mitigado por el régimen simplificado y la equivalencia SBS.

Riesgos: Escasez de auditores acreditados fuera de Lima; incumplimiento formal de EPS y hospitales regionales sin apoyo técnico; demoras en la calificación por reguladores.

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

- **Constitucional** — Con observaciones: Las obligaciones impuestas a operadores esenciales son restricciones proporcionales a la libertad de empresa (art. 59), justificadas por la protección de la vida, la salud y la seguridad. Debe atribuirse expresamente la potestad sancionadora y no dejar al Ejecutivo la ampliación ilimitada del ámbito subjetivo.
- **Técnica legislativa** — Observaciones graves: Las obligaciones son razonables y su articulación con los Activos Críticos Nacionales y la SBS es correcta, pero la ley no tipifica infracciones ni sanciones: remite a leyes de creación de reguladores que no contemplan estas conductas y a una «autoridad nacional de ciberseguridad» y una «ley de la materia» que no existen. Además, permite ampliar por decreto supremo el ámbito de un régimen de obligaciones.
- **Concordancia normativa** — Con observaciones: Normas verificadas (D.S. 106-2017-PCM, Res. SBS 504-2021, D.U. 007-2020, D.S. 126-2025-PCM). La lista de sectores esenciales duplica parcialmente el art. 9.1 del D.U. 007-2020 y la regla de supervisión choca con CIB-01. Debe fusionarse con CIB-01/CIB-03 o, al menos, compartir definiciones.
- **Seguridad** — Con observaciones: Obligaciones correctas y alineadas con prácticas internacionales (gestión de riesgos, alta dirección, auditorías, cadena de suministro) y con reserva adecuada de la lista de operadores. Faltan controles mínimos explícitos para tecnología operacional (sistemas de control industrial), la remisión a la notificación de incidentes es a una 'ley de la materia' inexistente, y el sistema de pagos tiene supervisor distinto de la SBS.

• **Derecho tecnológico** — Observaciones graves: La idea (listado legal de sectores y obligaciones proporcionales al estilo NIS2/SOCI) es correcta y usa bien la terminología del DS 126-2025-PCM (OSCD). Pero la supervisión queda en reguladores sectoriales sin habilitación sancionadora ni infracciones tipificadas, depende de una 'autoridad nacional de ciberseguridad' inexistente y omite que el art. 9.1 del DU 007-2020 ya obliga a casi los mismos sectores. Sin esas correcciones es inaplicable.

IV. Efecto de la vigencia de la norma

Modifica el numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020 (único catálogo de sectores); desarrolla su artículo 9; atribuye potestad sancionadora a los reguladores sectoriales (complementa sus leyes de creación sin modificarlas); complementa el Decreto Supremo 106-2017-PCM, la Ley 30224 (acreditación) y la Ley 29440 (sistemas de pagos); obliga a adecuar el Decreto Supremo 126-2025-PCM. No modifica la Ley 30999 ni la Ley 26702. No requiere votación de ley orgánica.

V. Indicador de éxito al 2031

A 2031, 100 % de los operadores calificados con auditoría bienal presentada y plan de continuidad probado; número de operadores por sector publicado anualmente.

Normas relacionadas

- Decreto Supremo 106-2017-PCM, Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales — <https://www.gob.pe/institucion/pcm/normas-legales/454348-106-2017-pcm>
- 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>
- 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>
- Ley 30999, Ley de Ciberdefensa (2019) — https://www3.congreso.gob.pe/Docs/DGP/DIDP/files/ley_30999.pdf

Antecedentes

Periodo 2021-2026 (según verificación en SPLEY del revisor normativo): PL 13568/2025-CR, que fortalece el sistema nacional de ciberseguridad para la protección de las infraestructuras críticas (en comisión); PL 09906/2024-CR, Ley de seguridad digital o ciberseguridad (con dictamen). Ninguno fue publicado como ley.

Referencias internacionales

- 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>
- Australia: Security of Critical Infrastructure Act 2018 — <https://www.legislation.gov.au/C2018A00029/latest/text>
- Chile: Ley 21.663, Ley Marco de Ciberseguridad (crea la Agencia Nacional de Ciberseguridad y CSIRT) — <https://www.bcn.cl/leychile/navegar?idNorma=1202434>
- 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

- Apaxi (07-09-2026): Normas de ciberseguridad para empresas en el Perú — <https://apaxi.info/2026/09/07/normas-ciberseguridad-empresas-peru/>
- gob.pe (DINI): Activos Críticos Nacionales (ACN) — <https://www.gob.pe/10400-activos-criticos-nacionales-acn>

- EY Perú: Reglamento del Marco de Confianza Digital (DS 126-2025-PCM) —
https://www.ey.com/es_pe/technical/tax-alert/reglamento-ley-marco-confianza-digital-medidas-fortalecimiento
- Texto del DS 126-2025-PCM (copia LP Derecho) —
<https://img.lpderecho.pe/wp-content/uploads/2025/11/Decreto-Supremo-126-2025-PCM-LPDerecho.pdf>

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/CIB-02.html>