

Ley que establece la ventanilla única y los plazos armonizados para la notificación obligatoria de incidentes de seguridad digital

Unifica en una ventanilla digital, soportada en el Registro Nacional de Incidentes de Seguridad Digital, la notificación de incidentes hoy dispersa entre el Centro Nacional de Seguridad Digital, la Autoridad Nacional de Protección de Datos Personales y los supervisores sectoriales; armoniza los plazos con las 48 horas vigentes (alerta temprana en 24 horas, notificación en 48 horas e informe final en 30 días), tipifica la omisión y protege la información notificada.

Comisión (Cámara de Diputados): Ciencia, Innovación Tecnológica y Sociedad Digital (+ Justicia y Derechos Humanos) ·

Revisora (Senado): En asuntos de Salud, Educación, Cultura, Mujer y Desarrollo Social y Digital · **Prioridad:** alta · **Costo fiscal:**

bajo · **Plazo:** corto

Plan Perú 2050: Ciber Seguridad, Transformación Digital

I. Exposición de motivos

Las organizaciones peruanas enfrentan regímenes paralelos de notificación de incidentes. El Decreto Supremo 126-2025-PCM (art. 32.1) exige notificar los incidentes de nivel crítico al Centro Nacional de Seguridad Digital en un plazo no mayor de 48 horas, y el Decreto Supremo 016-2024-JUS (art. 34.1) exige notificar los incidentes de seguridad de datos personales a la Autoridad Nacional de Protección de Datos Personales también en 48 horas, con contenidos mínimos distintos (El Peruano, 27-3-2026). Los supervisores sectoriales, como la SBS, mantienen sus propios canales de reporte. Los plazos para incidentes no críticos dependen aún de instrumentos pendientes de aprobación por la Secretaría de Gobierno y Transformación Digital. Un mismo evento puede requerir tres o más reportes con formatos distintos, lo que consume tiempo crítico durante la respuesta y genera información inconsistente. Además, la omisión de notificar no tiene una consecuencia tipificada con rango de ley fuera del ámbito de datos personales y de los sectores con regulación propia, y no existe una garantía legal expresa de que la información notificada no será usada para autoincriminar al notificante ni divulgada indebidamente, lo que desalienta el reporte. Sin datos consolidados, el país no puede medir tendencias ni emitir alertas oportunas.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE ESTABLECE LA VENTANILLA ÚNICA Y LOS PLAZOS ARMONIZADOS PARA LA NOTIFICACIÓN OBLIGATORIA DE INCIDENTES DE SEGURIDAD DIGITAL

Artículo 1. Objeto

La presente ley tiene por objeto establecer la ventanilla única de notificación de incidentes de seguridad digital, los plazos armonizados de notificación, las garantías aplicables a la información notificada y el régimen de infracciones por su incumplimiento.

Artículo 2. Sujetos obligados

2.1. Están obligados a notificar a través de la ventanilla única los sujetos comprendidos en el numeral 9.1 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.

2.2. Los demás titulares de bancos de datos personales pueden utilizar la ventanilla única para cumplir su obligación de notificación ante la Autoridad Nacional de Protección de Datos Personales.

Artículo 3. Ventanilla única

3.1. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital y del Centro Nacional de Seguridad Digital, o del órgano que haga sus veces, implementa la ventanilla única de notificación sobre la plataforma del Registro Nacional de Incidentes de Seguridad Digital previsto en el artículo 8 del Decreto de Urgencia 007-2020. La notificación efectuada a través de ella se tiene por cumplida ante la Autoridad Nacional de Protección de Datos Personales, la Superintendencia de Banca, Seguros y AFP, el

Banco Central de Reserva del Perú, los organismos reguladores y demás supervisores, a quienes la plataforma remite automáticamente la información de su competencia.

3.2. La plataforma cumple requisitos reforzados de seguridad: autenticación multifactor de los notificantes, cifrado de la información en tránsito y en reposo, segregación del acceso de cada supervisor a la información de su competencia, registro inalterable de accesos, alojamiento en infraestructura del Estado en territorio nacional y pruebas de seguridad independientes anuales. Se mantiene un canal alternativo de notificación fuera de banda para cuando la plataforma no esté disponible.

3.3. Todo reporte de incidentes de seguridad digital o de pagos derivados de extorsión informática exigido por ley se presenta a través de la ventanilla única.

Artículo 4. Plazos armonizados

4.1. Ante un incidente significativo, el sujeto obligado presenta:

- a) Una alerta temprana dentro de las veinticuatro horas de haber tomado conocimiento, indicando si se sospecha de un acto ilícito.
- b) Una notificación del incidente dentro de las cuarenta y ocho horas de haber tomado conocimiento, con evaluación inicial de gravedad, impacto e indicadores de compromiso.
- c) Un informe final dentro de los treinta días calendario, con causa raíz y medidas adoptadas.

4.2. La notificación del literal b) se presenta en un formulario único que integra los contenidos mínimos exigidos por todas las autoridades destinatarias, incluidos los de la normativa de protección de datos personales, y da por cumplidas las obligaciones de notificación previstas en el Decreto Supremo 126-2025-PCM y en el Decreto Supremo 016-2024-JUS.

4.3. Solo prevalecen los plazos menores que establezcan la Superintendencia de Banca, Seguros y AFP y el Banco Central de Reserva del Perú para sus supervisados.

Artículo 5. Incidente significativo

5.1. Se considera significativo el incidente que causa o puede causar una perturbación operativa grave del servicio, pérdidas económicas relevantes o daños materiales o inmateriales considerables a terceros.

5.2. La Clasificación de Incidentes de Seguridad Digital que aprueba la Secretaría de Gobierno y Transformación Digital establece qué niveles constituyen incidente significativo, con umbrales objetivos por sector. Los incidentes no significativos se registran en la ventanilla única en los plazos que dicha clasificación determine.

Artículo 6. Comunicación a afectados

Cuando el incidente pueda afectar derechos o intereses de los usuarios, el sujeto obligado les comunica, sin dilación indebida y por medios directos, la naturaleza del incidente y las medidas de protección recomendadas, conforme a la Ley 29733, Ley de Protección de Datos Personales, y su reglamento.

Artículo 7. Confidencialidad y uso de la información

7.1. La información notificada 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, y se utiliza para fines de respuesta, prevención, estadística y supervisión.

7.2. La notificación no constituye reconocimiento de responsabilidad. Los supervisores pueden iniciar procedimientos sancionadores por incumplimiento de deberes de seguridad sobre la base de su propia actividad de fiscalización, en la que pueden valorar la información notificada junto con otros medios probatorios; la información notificada no puede ser la única prueba de la infracción.

7.3. La confidencialidad no impide comunicar al Ministerio Público y a la Policía Nacional del Perú los hechos que revistan caracteres de delito. Cuando la alerta indique la sospecha de un delito, la plataforma ofrece al notificante la remisión directa a la Policía Nacional del Perú y al Ministerio Público, y el notificante preserva la evidencia digital relevante por noventa días. Los indicadores técnicos de compromiso se comparten con dichas instituciones; la información que identifique al notificante solo se entrega por requerimiento fiscal o mandato judicial conforme a ley.

7.4. Los incidentes que puedan afectar la seguridad nacional se comunican al Comando Conjunto de las Fuerzas Armadas conforme a la Ley 30999, Ley de Ciberdefensa.

Artículo 8. Retroalimentación, alertas e informe anual

8.1. El Centro Nacional de Seguridad Digital emite al notificante una respuesta inicial dentro de las veinticuatro horas siguientes a la alerta temprana y difunde alertas a otros sujetos potencialmente afectados, omitiendo cualquier dato que permita identificar al notificante, salvo su consentimiento.

8.2. El Centro Nacional de Seguridad Digital publica un informe anual con estadísticas agregadas y anonimizadas de incidentes por sector, tipo y región, en formato de datos abiertos.

Artículo 9. Infracciones, sanciones y autoridad competente

9.1. Constituye infracción grave no presentar la alerta temprana, la notificación o el informe final dentro de los plazos del artículo 4. Constituye infracción muy grave presentar información falsa u ocultar un incidente significativo.

9.2. Las infracciones graves se sancionan 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, graduadas conforme al numeral 3 del artículo 248 del Texto Único Ordenado de la Ley 27444, aprobado por el Decreto Supremo 006-2026-JUS.

9.3. Sanciona el organismo regulador o supervisor sectorial competente y, en su defecto, la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno y Transformación Digital. La Autoridad Nacional de Protección de Datos Personales mantiene su potestad sancionadora conforme a la Ley 29733. En ningún caso se sanciona dos veces el mismo hecho con identidad de sujeto y fundamento.

9.4. En las entidades públicas, el incumplimiento constituye falta disciplinaria de los servidores responsables conforme a la Ley 30057, Ley del Servicio Civil.

Primera. Disposición Complementaria Final

Reglamentación y adecuación. El Poder Ejecutivo, mediante decreto supremo refrendado por el presidente del Consejo de Ministros y el ministro de Justicia y Derechos Humanos, reglamenta la presente ley en un plazo no mayor de noventa días hábiles contados a partir del día siguiente de su publicación, y adecúa los artículos 29 a 34 del Decreto Supremo 126-2025-PCM y el artículo 34 del Decreto Supremo 016-2024-JUS.

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.

Única. Disposición Complementaria Transitoria

Implementación de la ventanilla única. La ventanilla única se implementa en un plazo de doce meses contados a partir de la entrada en vigencia del reglamento. Mientras tanto, rigen los canales vigentes, y las obligaciones y sanciones de los artículos 4 y 9 son exigibles desde la puesta en operación de la ventanilla.

Única. Disposición Complementaria Modificatoria

Incorporación del numeral 8.4 al artículo 8 del Decreto de Urgencia 007-2020. Se incorpora el numeral 8.4 al artículo 8 del Decreto de Urgencia 007-2020, en los términos siguientes:

«Artículo 8. Registro Nacional de Incidentes de Seguridad Digital
[...]

8.4. El Registro Nacional de Incidentes de Seguridad Digital soporta la ventanilla única de notificación de incidentes de seguridad digital prevista en la ley de la materia.»

III. Análisis costo-beneficio

Gasto público bajo: la plataforma del Registro Nacional de Incidentes ya existe y se amplía con interoperabilidad hacia los supervisores y requisitos reforzados de seguridad; el editor estima un costo de S/ 1,5 a 3 millones en desarrollo y S/ 0,5 a 1 millón anual de operación y pruebas de seguridad, con cargo al presupuesto de la PCM. Para las empresas, reduce costos de cumplimiento al sustituir varios reportes por un formulario único. Los plazos se armonizan con las 48 horas vigentes, por lo que no se imponen cargas nuevas; la alerta temprana de 24 horas mejora la respuesta coordinada. El beneficio principal es contar con datos consolidados para alertas tempranas y política pública. La confidencialidad incentiva el reporte, sin restar capacidad sancionadora frente a la omisión ni impedir la persecución penal.

Normas que modifica

- Decreto de Urgencia 007-2020, Marco de Confianza Digital, art. 8, num. 8.4 — *incorpora*
- Decreto Supremo 126-2025-PCM, arts. 29 a 34 — *complementa*
- Decreto Supremo 016-2024-JUS, Reglamento de la Ley 29733, art. 34 — *complementa*
- Texto Único Ordenado de la Ley 27806, art. 17, num. 6 (por remisión) — *complementa*

Entidades implicadas (quién hace qué)

- **PCM-SGTD / CNSD** (ejecutora): Implementa y asegura la ventanilla única (art. 3), aprueba la clasificación de incidentes (art. 5.2), emite alertas e informe anual (art. 8) y sanciona en defecto de supervisor (art. 9.3).
- **ANPD** (supervisora): Recibe automáticamente los incidentes con datos personales y conserva su potestad sancionadora (arts. 3.1 y 9.3).
- **Supervisores** (sancionadora): Reciben la información de su competencia y sancionan la omisión de notificar de sus supervisados (arts. 3.1, 4.3 y 9.3).
- **MP / PNP** (beneficiaria): Reciben la remisión de incidentes con sospecha de delito e indicadores de compromiso (art. 7.3).
- **CCFFAA** (consultiva): Recibe incidentes que afecten la seguridad nacional (art. 7.4).
- **MINJUSDH** (reglamentadora): Corefrenda el reglamento y adecúa el D.S. 016-2024-JUS (DCF Primera).

Sujetos obligados: Sujetos del numeral 9.1 del artículo 9 del D.U. 007-2020: entidades públicas y proveedores de servicios digitales de finanzas, servicios básicos, salud, transporte de personas, internet, actividades críticas y educación. Uso voluntario para los demás titulares de bancos de datos personales.

Beneficiarios: Sujetos obligados (menos reportes duplicados), usuarios afectados por incidentes (comunicación directa) y organizaciones que reciben alertas tempranas. No cuantificable con información pública.

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

Tipo: mixto

Costo para el Estado: S/ 1,5–3 millones (desarrollo, único) y S/ 0,5–1 millón/año (operación y pruebas de seguridad), estimación del editor

Horizonte: 2027-2029 desarrollo; anual desde 2029

Financiamiento: Presupuesto institucional de la PCM sin demandar recursos adicionales al Tesoro Público; si se requieren recursos adicionales, coordinación con el Poder Ejecutivo e informe previo de sostenibilidad fiscal del MEF antes del dictamen.

Supuestos: Ampliación de la plataforma existente del Registro Nacional de Incidentes con formulario único, interoperabilidad con 6 a 8 supervisores, canal alternativo y prueba de penetración independiente anual. Costos unitarios supuestos por el editor a partir de proyectos de software público de escala comparable; sin fuente oficial.

Beneficio para el Estado: Datos consolidados para política pública y alertas tempranas; menor carga de gestión de reportes en ANPD y supervisores. No cuantificable con información pública.

Beneficio para la sociedad: Ahorro de costos de cumplimiento al sustituir varios reportes por uno; comunicación oportuna a usuarios afectados. No cuantificable con información pública.

Inversión privada: No aplica.

Costo para privados: Bajo: los plazos coinciden con las 48 horas vigentes; se añade la alerta temprana de 24 horas y el informe final a 30 días.

Riesgos: Concentración de información sensible en una sola plataforma (mitigado con requisitos reforzados del art. 3.2 y canal alternativo); retrasos en la interoperabilidad con supervisores; resistencia de supervisores a abandonar canales propios.

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

- **Constitucional** — Conforme: La ventanilla única y los plazos escalonados son constitucionalmente inobjetables; la garantía de no utilizar la notificación como única prueba protege el derecho a no autoincriminarse en sede administrativa. Solo debe aclararse que

la confidencialidad no impide la persecución penal.

- **Técnica legislativa** — Con observaciones: La ventanilla única y los plazos escalonados están bien diseñados y reducen cargas, pero la obligación de notificar no tiene consecuencia jurídica tipificada y la garantía de confidencialidad no se articula con la potestad sancionadora de la ANPD y la SBS por fallas de seguridad. Hay además errores formales en plazos y disposiciones.
- **Concordancia normativa** — Con observaciones: Diagnóstico verificado: D.S. 126-2025-PCM art. 32.1 (48 h para incidentes críticos al CNSD) y D.S. 016-2024-JUS art. 34.1 (48 h a la ANPD). La ventanilla única es útil, pero la regla 'prevalece el plazo menor' deja los 72 h sin aplicación práctica para incidentes críticos, y debe articularse con CIB-01, CIB-02, CIB-13 y CIB-14, que crean canales o reportes propios.
- **Seguridad** — Con observaciones: Excelente orientación (ventanilla única, escalonamiento 24h/72h/30 días, confidencialidad e inmunidad de uso). Pero la cláusula de prevalencia del plazo menor anula el escalonamiento frente a los 48 horas del DS 126-2025-PCM y del DS 016-2024-JUS, y la plataforma única concentra información extremadamente sensible de todos los operadores sin requisitos de seguridad ni canal alternativo.
- **Derecho tecnológico** — Con observaciones: Propuesta muy útil: la doble notificación CNSD/ANPD (ambas en 48 h, arts. 32.1 DS 126-2025-PCM y 34.1 DS 016-2024-JUS) es una carga real y el esquema 24h/72h/30 días replica NIS2 y CIRCIA correctamente. Debe armonizar 'incidente significativo' con la clasificación por niveles del DS 126-2025-PCM, aclarar que el plazo de 48 h de la ANPD prevalece para datos personales, unificar los contenidos mínimos y blindar la confidencialidad con la técnica del art. 17 del TUO de la Ley 27806.

IV. Efecto de la vigencia de la norma

Incorpora el numeral 8.4 al artículo 8 del Decreto de Urgencia 007-2020; complementa su artículo 9 y la Ley 29733 en cuanto al canal de notificación; declara la confidencialidad conforme al numeral 6 del artículo 17 del TUO de la Ley 27806; obliga a adecuar los artículos 29 a 34 del Decreto Supremo 126-2025-PCM y el artículo 34 del Decreto Supremo 016-2024-JUS. Mantiene los plazos menores fijados por la SBS y el BCRP. No requiere votación de ley orgánica.

V. Indicador de éxito al 2031

A 2028, ventanilla única operativa e interoperable con ANPD, SBS, BCRP y OSIPTEL, con prueba de seguridad independiente anual publicada en resumen; desde 2028, informe anual de incidentes publicado en datos abiertos.

Normas relacionadas

- 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 Supremo 016-2024-JUS, Reglamento de la Ley 29733 — https://www3.congreso.gob.pe/Docs/DGP/DIDP/files/ds_016-2024-jus.pdf
- Ley 29733, Ley de Protección de Datos Personales — <https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf>
- 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>
- 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

Antecedentes

Según verificación en SPLEY del revisor normativo, no se identificaron proyectos del periodo 2021-2026 específicos sobre notificación única de incidentes. Relacionados: PL 09906/2024-CR, Ley de seguridad digital o ciberseguridad (con dictamen), y PL 14045/2025-CR, responsabilidad administrativa de personas jurídicas frente a delitos informáticos y vulneraciones de datos (en comisión).

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>
- Estados Unidos: Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) — <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>
- Chile: Ley 21.663, Ley Marco de Ciberseguridad (crea la Agencia Nacional de Ciberseguridad y CSIRT) — <https://www.bcn.cl/leychile/navegar?idNorma=1202434>

Fuentes

- El Peruano (27-03-2026): Incidente de seguridad digital o de datos personales — doble régimen de notificación — <https://elperuano.pe/noticia/292188-incidente-de-seguridad-digital-o-de-datos-personales>
- Decreto Supremo 126-2025-PCM (El Peruano) — <https://busquedas.elperuano.pe/dispositivo/EX/2455024-1>
- Decreto Supremo 016-2024-JUS (copia del Congreso) — https://www3.congreso.gob.pe/Docs/DGP/DIDP/files/ds_016-2024-jus.pdf
- gob.pe: Reportar incidentes de seguridad digital (Centro Nacional de Seguridad Digital) — <https://www.gob.pe/14084-reportar-incidentes-de-seguridad-digital>

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/CIB-03.html>