

Ley que promueve la ciberresiliencia de las mipymes, regula la transparencia de los seguros de riesgo cibernético y establece el reporte obligatorio de pagos por extorsión informática

Promueve la ciberresiliencia de las mipymes mediante un programa de autodiagnóstico y controles básicos y un sello verificable sin puntaje automático en contrataciones; establece reglas de transparencia y de oponibilidad de exclusiones para los seguros de riesgo cibernético que se contraten o renueven; obliga a reportar los pagos por extorsión informática a través del canal nacional de notificación de incidentes, con infracción tipificada; y prohíbe el pago de rescates con fondos públicos, con una excepción controlada ante riesgo para la vida.

Comisión (Cámara de Diputados): Producción, Comercio Exterior y Turismo (+ Economía, Banca, Finanzas e Inteligencia Financiera) · **Revisora (Senado):** En asuntos de Desarrollo Productivo, Energía y Minas, Infraestructura y Trabajo · **Prioridad:** media · **Costo fiscal:** bajo · **Plazo:** corto
Plan Perú 2050: Mipymes, Seguros, Ciber Seguridad

I. Exposición de motivos

Las micro y pequeñas empresas son blanco frecuente de fraude y ransomware, pero rara vez cuentan con personal o presupuesto de ciberseguridad. El mercado de seguros de riesgo cibernético en el Perú es incipiente y sus pólizas suelen contener exclusiones complejas (guerra, actos de Estado, falta de parches) que el asegurado pyme no comprende, lo que genera disputas al momento del siniestro; la Ley 29946, Ley del Contrato de Seguro, y la normativa de conducta de mercado de la SBS establecen reglas generales de transparencia, pero no estándares específicos para este ramo. Además, el país no tiene información sobre cuántas organizaciones pagan rescates ni cuánto: el Decreto Supremo 126-2025-PCM regula la notificación de incidentes, no los pagos de extorsión, lo que impide dimensionar el financiamiento que reciben las bandas criminales y orientar la persecución penal y la inteligencia financiera. Australia estableció en su Cyber Security Act 2024 el reporte obligatorio de pagos de ransomware en 72 horas para empresas por encima de un umbral de facturación. No se dispone de cifras oficiales peruanas de pagos de rescate ni de penetración del ciberseguro. Las tres medidas comparten un mismo objeto, la gestión del riesgo económico del ciberdelito en las empresas, lo que justifica su tratamiento conjunto.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE PROMUEVE LA CIBERRESILIENCIA DE LAS MIPYMES, REGULA LA TRANSPARENCIA DE LOS SEGUROS DE RIESGO CIBERNÉTICO Y ESTABLECE EL REPORTE OBLIGATORIO DE PAGOS POR EXTORSIÓN INFORMÁTICA

Artículo 1. Objeto

La presente ley tiene por objeto reducir el riesgo económico del ciberdelito en las empresas mediante la promoción de la ciberresiliencia de las micro, pequeñas y medianas empresas, reglas de transparencia para los seguros de riesgo cibernético y la obligación de reportar los pagos efectuados por extorsión informática.

Artículo 2. Programa de ciberresiliencia mipyme

El Ministerio de la Producción, en coordinación con la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital y del Centro Nacional de Seguridad Digital, implementa, con cargo a su presupuesto institucional y en el marco de sus programas existentes, un programa gratuito de autodiagnóstico en línea, guías de controles básicos (copias de seguridad, autenticación multifactor, actualizaciones y gestión de accesos) y capacitación para mipymes, a través de los Centros de Desarrollo Empresarial y de plataformas digitales.

Artículo 3. Sello de controles básicos

3.1. Las mipymes que acrediten la implementación de los controles básicos pueden obtener un sello de ciberresiliencia, que se otorga previa verificación documental y revisión aleatoria por muestreo a cargo del Ministerio de la Producción o de terceros autorizados, con vigencia de dos años y revocable.

3.2. La declaración falsa conlleva la pérdida del sello y se considera información inexacta para efectos de la normativa de contrataciones públicas.

3.3. El Reglamento de la Ley 32069, Ley General de Contrataciones Públicas, puede considerar el sello como factor de evaluación facultativo en contrataciones que impliquen tratamiento de datos personales, reconociendo como equivalentes las certificaciones de seguridad de la información de estándar internacional que acrediten los demás postores.

Artículo 4. Transparencia de los seguros de riesgo cibernético

Las empresas de seguros que comercialicen coberturas de riesgo cibernético entregan al contratante un resumen estandarizado de máximo dos páginas que detalle coberturas, exclusiones, deducibles, obligaciones de seguridad exigidas al asegurado y procedimiento ante siniestros, conforme al formato que apruebe la Superintendencia de Banca, Seguros y AFP, en concordancia con la Ley 29946 y la normativa de conducta de mercado del sistema de seguros.

Artículo 5. Oponibilidad de exclusiones

En los seguros de riesgo cibernético, las exclusiones por falta de medidas de seguridad solo son oponibles si la medida exigida fue expresamente detallada en el resumen estandarizado y guarda relación causal con el siniestro. Corresponde a la empresa de seguros acreditar dicha relación causal.

Artículo 6. Reporte de pagos por extorsión informática

6.1. Las personas jurídicas con ingresos anuales superiores a mil setecientas unidades impositivas tributarias, las entidades públicas, las empresas del Estado y los sujetos comprendidos en el numeral 9.1 del artículo 9 del Decreto de Urgencia 007-2020 que efectúen, directamente o a través de terceros, un pago o transferencia de valor en respuesta a una extorsión informática, lo reportan dentro de las setenta y dos horas siguientes al pago, indicando monto, medio de pago y datos del extorsionador disponibles.

6.2. El reporte se presenta a través del canal nacional de notificación de incidentes de seguridad digital administrado por la Presidencia del Consejo de Ministros, como información complementaria de la notificación del incidente que lo originó.

6.3. El reporte no sustituye la denuncia penal ni las obligaciones de reporte de operaciones sospechosas de los sujetos obligados ante la Unidad de Inteligencia Financiera del Perú.

Artículo 7. Confidencialidad y uso del reporte

La información reportada es 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. Se utiliza con fines de inteligencia de amenazas, estadística y apoyo a la investigación penal, y se comparte con el Ministerio Público y con la Unidad de Inteligencia Financiera del Perú en el marco de sus competencias y de la Ley 27693. El reporte no constituye por sí mismo prueba de infracción del reportante.

Artículo 8. Prohibición de pago con fondos públicos

8.1. Las entidades de la administración pública y las empresas del Estado no pueden pagar rescates por extorsión informática con fondos públicos.

8.2. Excepcionalmente, cuando exista riesgo inminente para la vida o la salud de las personas y se haya acreditado la inexistencia de alternativa técnica de recuperación, el pago puede autorizarse por resolución del titular del sector correspondiente, con informe previo del Centro Nacional de Seguridad Digital y comunicación inmediata a la Contraloría General de la República, al Ministerio Público y a la Unidad de Inteligencia Financiera del Perú.

8.3. El pago efectuado en contravención de este artículo genera responsabilidad administrativa funcional y constituye falta muy grave conforme a la Ley 30057, Ley del Servicio Civil.

Artículo 9. Infracciones y autoridad competente

9.1. Constituye infracción grave la omisión del reporte del artículo 6 por personas jurídicas privadas, sancionable con multa de hasta cincuenta unidades impositivas tributarias por el organismo regulador o

supervisor sectorial competente y, en su defecto, por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, conforme al numeral 3 del artículo 248 del Texto Único Ordenado de la Ley 27444, aprobado por el Decreto Supremo 006-2026-JUS. En entidades públicas y empresas del Estado, la omisión constituye falta disciplinaria conforme a la Ley 30057.

9.2. El incumplimiento del artículo 4 por las empresas de seguros es sancionable por la Superintendencia de Banca, Seguros y AFP conforme a su régimen de infracciones y sanciones.

Artículo 10. Estadística pública

La Presidencia del Consejo de Ministros publica anualmente estadísticas agregadas y anonimizadas de los pagos reportados, y la Superintendencia de Banca, Seguros y AFP publica la evolución de primas y siniestros del ramo de riesgo cibernético.

Primera. Disposición Complementaria Final

Reglamentación. El Poder Ejecutivo, mediante decreto supremo refrendado por el ministro de la Producción, el ministro de Economía y Finanzas y el presidente del Consejo de Ministros, previa opinión de la Superintendencia de Banca, Seguros y AFP, 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

Financiamiento. La implementación de la presente ley se financia con cargo al presupuesto institucional del Ministerio de la Producción y de la Presidencia del Consejo de Ministros, sin demandar recursos adicionales al Tesoro Público.

Única. Disposición Complementaria Transitoria

Exigibilidad y aplicación temporal. La obligación del artículo 6 es exigible a los seis meses y la del artículo 4 a los doce meses de la publicación del reglamento. Los artículos 4 y 5 se aplican a los contratos de seguro que se celebren o renueven a partir de su exigibilidad.

III. Análisis costo-beneficio

Costo fiscal bajo: el programa mipyme se apoya en los Centros de Desarrollo Empresarial y plataformas existentes de PRODUCE, y el editor estima S/ 1 a 3 millones anuales para contenidos, verificación por muestreo y capacitación; la SBS regula el resumen estandarizado dentro de sus funciones y el reporte de pagos se integra al canal de notificación existente. Para las aseguradoras, el costo es documental y se aplica solo a pólizas nuevas o renovadas. El reporte de pagos impone una carga mínima a empresas medianas y grandes y genera información inédita para dimensionar el financiamiento criminal y orientar la persecución penal y la inteligencia financiera. La prohibición de pagar rescates con fondos públicos evita incentivar ataques contra el Estado; la excepción controlada ante riesgo para la vida evita dejar al funcionario sin regla en casos extremos.

Normas que modifica

- Ley 29946, Ley del Contrato de Seguro, reglas especiales del ramo cibernético (arts. 4 y 5 de la ley) — *complementa*
- Ley 32069, Ley General de Contrataciones Públicas, y su reglamento, factor de evaluación facultativo — *complementa*
- Ley 27693, Ley que crea la Unidad de Inteligencia Financiera del Perú, recepción de información — *complementa*
- Decreto de Urgencia 007-2020 y Decreto Supremo 126-2025-PCM, canal de notificación (reporte complementario) — *complementa*

Entidades implicadas (quién hace qué)

- **PRODUCE** (ejecutora): Implementa el programa mipyme y otorga y verifica el sello (arts. 2 y 3).
- **PCM-SGTD / CNSD** (sancionadora): Recibe los reportes de pagos, informa sobre excepciones de pago, publica estadística y sanciona en defecto de supervisor (arts. 6, 8.2, 9.1 y 10).
- **SBS** (reguladora): Aprueba el formato de resumen, sanciona su incumplimiento y publica estadística del ramo (arts. 4, 9.2 y 10).
- **UIF / MP** (beneficiaria): Reciben la información de pagos y las comunicaciones de pagos excepcionales (arts. 7 y 8.2).

- **CGR** (supervisora): Recibe la comunicación de pagos excepcionales con fondos públicos (art. 8.2).

Sujetos obligados: Personas jurídicas con ingresos anuales superiores a 1 700 UIT, entidades públicas, empresas del Estado y sujetos del numeral 9.1 del art. 9 del D.U. 007-2020 (reporte de pagos); empresas de seguros que comercialicen el ramo cibernético; mipymes que soliciten el sello.

Beneficiarios: Mipymes que acceden al programa gratuito y asegurados del ramo cibernético; Ministerio Público y UIF por la información de pagos. No cuantificable con información pública.

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

Tipo: gasto

Costo para el Estado: S/ 1–3 millones/año (estimación del editor)

Horizonte: anual, desde 2028

Financiamiento: Presupuesto institucional de PRODUCE y de la PCM, en el marco de programas existentes, sin demandar recursos adicionales al Tesoro Público.

Supuestos: Contenidos y plataforma de autodiagnóstico, verificación por muestreo del sello y capacitación a través de los Centros de Desarrollo Empresarial existentes de PRODUCE; el reporte de pagos se integra al canal de notificación de la PCM sin desarrollo independiente. Costos supuestos por el editor, sin fuente oficial.

Beneficio para el Estado: Información inédita sobre pagos de rescate para la persecución penal y la inteligencia financiera; desincentivo a los ataques contra entidades públicas. No cuantificable con información pública.

Beneficio para la sociedad: Menos incidentes en mipymes por controles básicos de bajo costo y menos disputas en siniestros de ciberseguros. No cuantificable con información pública.

Inversión privada: Desarrollo del mercado de ciberseguros y de servicios de seguridad para mipymes; no cuantificable con información pública.

Costo para privados: Reporte de pagos (carga mínima para medianas y grandes empresas); costo documental para aseguradoras; costo voluntario de las mipymes que busquen el sello.

Riesgos: Subreporte de pagos por temor reputacional (mitigado por la confidencialidad); declaraciones falsas para obtener el sello (mitigado por muestreo y revocación); uso indebido de la excepción de pago (mitigado por comunicación a la CGR, el MP y la UIF).

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

- **Constitucional** — Con observaciones: Las medidas son en general compatibles con la Constitución. Deben corregirse el sello como factor de evaluación reservado a mipymes, que trata desigualmente a postores en contrataciones (arts. 2.2 y 76), la falta de consecuencia jurídica del deber de reporte y la aplicación temporal de las reglas sobre pólizas (art. 62).
- **Técnica legislativa** — Con observaciones: La propuesta combina tres materias (programa mipyme, transparencia de seguros y reporte de pagos de rescate) y pone en riesgo el principio de unidad de materia. Además, la regla sobre exclusiones de seguros debe limitarse a contratos futuros por el art. 62 de la Constitución, y la obligación de reporte carece de consecuencia jurídica.
- **Concordancia normativa** — Con observaciones: Normas citadas correctas (Ley 29946, Contrato de Seguro; D.U. 007-2020; D.S. 126-2025-PCM). El reporte de pagos por extorsión crea un tercer canal y plazo (72 h al CNSD) que contradice la ventanilla única y los plazos de CIB-03; el 'sello' como factor de evaluación requiere modificar la Ley 32069 o su reglamento.
- **Seguridad** — Con observaciones: Combinación útil de apoyo a mipymes, transparencia en seguros y reporte de pagos de extorsión. La prohibición absoluta de pagar rescates con fondos públicos no prevé el caso extremo de riesgo para la vida (p. ej., hospitales), el sello basado en autodiagnóstico es fácilmente manipulable si pondera en contrataciones, y el reporte de pagos debe integrarse a la ventanilla única de incidentes.
- **Derecho tecnológico** — Con observaciones: Combina tres medidas razonables: programa mipyme, transparencia del ciberseguro y reporte de pagos de rescate (Australia, Cyber Security Act 2024, 72 h, correctamente citado). Ajustes: el 'sello' por autodiagnóstico tiene bajo nivel de aseguramiento y no debería puntuar en contrataciones sin verificación; la prohibición absoluta de pagar rescates con fondos públicos requiere una válvula para riesgo a la vida; y la categoría 'operadores de servicios esenciales' no está definida.

IV. Efecto de la vigencia de la norma

Ley autónoma que complementa la Ley 29946 (transparencia y exclusiones en el ramo cibernético, solo para contratos futuros), la Ley 32069 y su reglamento (factor de evaluación facultativo), la Ley 27693 (UIF-Perú), la Ley 30057, la Ley 30096, el Decreto de Urgencia 007-2020 y el Decreto Supremo 126-2025-PCM; declara la confidencialidad conforme al numeral 6 del artículo 17 del TUO de la Ley 27806. No modifica la Ley 26702. No requiere votación de ley orgánica.

V. Indicador de éxito al 2031

A 2031, al menos 50 000 mipymes con autodiagnóstico completado y estadística anual de pagos por extorsión informática y del ramo de ciberseguros publicada.

Normas relacionadas

- Ley 29946, Ley del Contrato de Seguro — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/29946.pdf>
- Ley 30096, Ley de Delitos Informáticos (2013) — <https://leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf>
- 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>

Antecedentes

Según verificación en SPLEY del revisor normativo, no se identificaron proyectos del periodo 2021-2026 sobre seguros cibernéticos, reporte de pagos por ransomware o ciberresiliencia mipyme.

Referencias internacionales

- Australia: Cyber Security Act 2024 (incluye reporte obligatorio de pagos de ransomware) — <https://www.legislation.gov.au/C2024A00098>
- Estados Unidos: NIST Cybersecurity Framework 2.0 — <https://www.nist.gov/cyberframework>
- 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>

Fuentes

- Apaxi (07-09-2026): Normas de ciberseguridad para empresas en el Perú — <https://apaxi.info/2026/09/07/normas-ciberseguridad-empresas-peru/>
- 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>
- CiberLATAM: Perú avanza con ciberseguridad sin ley general — <https://ciberlatam.com/noticias/peru-avanza-ciberseguridad-ley-general>

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/CIB-14.html>