

Ley que modifica la Ley 30096, Ley de Delitos Informáticos, y el Código Penal para tipificar la extorsión informática, comprender el material sintético en el chantaje sexual y sancionar la toma fraudulenta de líneas móviles

Incorpora a la Ley 30096 el delito de extorsión informática (ransomware) con pena no menor que la extorsión común y con exclusión expresa de la divulgación coordinada de vulnerabilidades de buena fe; amplía el artículo 9-A (Ley 32451) a la obtención fraudulenta de duplicados, reposición o portabilidad de líneas móviles; precisa que el chantaje sexual del artículo 176-C del Código Penal comprende el material generado sintéticamente; incorpora el numeral 6 al artículo 11; y regula la conservación rápida de datos sin acceso a contenido sin mandato judicial, conforme al Convenio de Budapest.

Comisión (Cámara de Diputados): Justicia y Derechos Humanos (+ Defensa Nacional y Orden Interno) · **Revisora (Senado):**

Justicia y Derechos Humanos · **Prioridad:** alta · **Costo fiscal:** nulo · **Plazo:** corto

Plan Perú 2050: Orden Público y Seguridad, Ciber Seguridad, Reforma Judicial

I. Exposición de motivos

La Ley 30096 tipifica el acceso ilícito, los atentados contra datos y sistemas, el fraude informático y la suplantación de identidad, y ha sido modificada, entre otras, por la Ley 30171, el Decreto Legislativo 1591 (2023), la Ley 32314 (2025), que incorporó el numeral 5 del artículo 11 (agravante por uso de inteligencia artificial), la Ley 32451 (2025), que incorporó el artículo 9-A (activación de SIM o línea móvil sin consentimiento del titular), y los Decretos Legislativos 1700 y 1741 (2026), sobre tráfico ilícito de datos (artículo 12-A). Persisten vacíos: el secuestro de datos mediante ransomware se procesa de forma fragmentada entre el atentado contra datos (artículo 3) y la extorsión del Código Penal, sin tipo que describa la conducta informática; la obtención fraudulenta del duplicado, la reposición o la portabilidad de una línea ajena, puerta de entrada al vaciado de cuentas, no está comprendida expresamente en el artículo 9-A, que solo sanciona la activación; y el chantaje sexual del artículo 176-C del Código Penal no menciona el material generado sintéticamente. Según información del Ministerio Público difundida por El Peruano (2-9-2026), entre enero y julio de 2026 se registraron 19 602 denuncias por fraude informático y 7 431 por suplantación de identidad. El Perú es parte del Convenio de Budapest (Resolución Legislativa 30913). Esta propuesta ciudadana sirve como referencia para el debate de la delegación de facultades en trámite (Proposición 0098-2026-2031-CD).

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE MODIFICA LA LEY 30096, LEY DE DELITOS INFORMÁTICOS, Y EL CÓDIGO PENAL PARA TIPIFICAR LA EXTORSIÓN INFORMÁTICA, COMPRENDER EL MATERIAL SINTÉTICO EN EL CHANTAJE SEXUAL Y SANCIONAR LA TOMA FRAUDULENTE DE LÍNEAS MÓVILES

Artículo 1. Objeto

La presente ley tiene por objeto modificar la Ley 30096, Ley de Delitos Informáticos, y el Código Penal, aprobado por el Decreto Legislativo 635, a fin de tipificar la extorsión informática, ampliar el delito de toma fraudulenta de líneas móviles, comprender el material sintético en el delito de chantaje sexual, incorporar una agravante por pluralidad de víctimas y regular la conservación rápida de datos informáticos.

Artículo 2. Incorporación del artículo 4-A a la Ley 30096

Se incorpora el artículo 4-A a la Ley 30096, Ley de Delitos Informáticos, en los términos siguientes:

«Artículo 4-A. Extorsión informática

El que, mediante el cifrado, bloqueo, sustracción o amenaza de divulgación de datos informáticos o la inutilización de un sistema informático, exige a la víctima o a un tercero una ventaja patrimonial, de naturaleza sexual o cualquier otra ventaja indebida para restablecer el acceso, devolver los datos o abstenerse de divulgarlos, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años.

La pena será no menor de quince ni mayor de veinticinco años cuando el hecho afecte servicios de salud, agua, energía, telecomunicaciones, servicios de emergencia u otros servicios esenciales, o a entidades de la administración pública.

Si el hecho constituye un delito más grave, se aplica la pena de este.

No constituye este delito la comunicación de una vulnerabilidad realizada de buena fe conforme al régimen de divulgación coordinada de vulnerabilidades, ni la solicitud de corrección antes de su publicación, ni la solicitud de la recompensa ofrecida por el titular del sistema.»

Artículo 3. Modificación del artículo 9-A de la Ley 30096

Se modifica el artículo 9-A de la Ley 30096, Ley de Delitos Informáticos, incorporado por la Ley 32451, en los términos siguientes:

«Artículo 9-A. Activación o toma fraudulenta de una SIM Card o de una línea de servicio móvil sin consentimiento del titular

El que, sin consentimiento del titular o empleando datos falsos o erróneos, activa una SIM Card o una línea de servicio móvil, o mediante engaño, suplantación o uso de documentos o datos de identidad ajenos obtiene el duplicado, la reposición, la portabilidad o el cambio de titularidad de una línea de servicio móvil de un tercero, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme al numeral 4 del artículo 36 del Código Penal.

Si el agente es trabajador o contratista de la empresa operadora o de su red de distribución, la pena será no menor de seis ni mayor de diez años e inhabilitación conforme al artículo 36 del Código Penal.

Si el agente, mediante la línea obtenida, comete además fraude informático u otro delito, se aplican las reglas del concurso real.»

Artículo 4. Incorporación del numeral 6 al artículo 11 de la Ley 30096

Se incorpora el numeral 6 al artículo 11 de la Ley 30096, Ley de Delitos Informáticos, cuyo numeral 5 fue incorporado por la Ley 32314, en los términos siguientes:

«Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

[...]

6. El delito se comete contra una pluralidad de víctimas mediante campañas automatizadas o afecta a personas adultas mayores o en situación de vulnerabilidad.»

Artículo 5. Incorporación de un párrafo al artículo 176-C del Código Penal

Se incorpora un último párrafo al artículo 176-C del Código Penal, aprobado por el Decreto Legislativo 635, en los términos siguientes:

«Artículo 176-C. Chantaje sexual

[...]

Las imágenes, materiales audiovisuales o audios a que se refiere el presente artículo comprenden los reales y los generados o alterados mediante tecnologías digitales, incluida la inteligencia artificial, que representen de manera verosímil a la víctima. Si la víctima es menor de dieciocho años, la pena será no menor de diez ni mayor de quince años e inhabilitación. Si el agente exige además una ventaja patrimonial o el hecho constituye un delito más grave, se aplica la pena de este.»

Artículo 6. Decomiso de activos virtuales

En los delitos previstos en la Ley 30096 y en el artículo 176-C del Código Penal, el juez puede ordenar la incautación y el decomiso de activos virtuales y su conversión, conforme al Código Procesal Penal, aprobado por el Decreto Legislativo 957, y al Decreto Legislativo 1373, sobre extinción de dominio, para la reparación de las víctimas.

Artículo 7. Conservación rápida de datos informáticos

7.1. El Ministerio Público y la Policía Nacional del Perú, como puntos de contacto de la red 24/7 prevista en el artículo 35 del Convenio sobre la Ciberdelincuencia, aprobado por la Resolución Legislativa 30913, pueden requerir a los proveedores de servicios la conservación rápida de datos informáticos específicos, incluidos los

de tráfico, conforme al artículo 16 de dicho Convenio, por un plazo de hasta noventa días, prorrogable por única vez por orden judicial.

7.2. La conservación no habilita el acceso a los datos ni su entrega, que requieren mandato judicial conforme al numeral 10 del artículo 2 de la Constitución Política del Perú y al Código Procesal Penal. El proveedor guarda reserva del requerimiento.

7.3. Lo dispuesto en el presente artículo es sin perjuicio de las obligaciones de conservación previstas en el Decreto Legislativo 1182.

Primera. Disposición Complementaria Final

Adecuación de protocolos. El Ministerio Público y la Policía Nacional del Perú adecúan sus protocolos de investigación en un plazo de noventa días hábiles contados a partir del día siguiente de la publicación de la presente ley.

Segunda. Disposición Complementaria Final

Estadística. El Ministerio Público incluye en su boletín estadístico la desagregación de denuncias por los tipos penales incorporados o modificados por la presente ley.

Tercera. Disposición Complementaria Final

Prevención de la toma de líneas. El Organismo Supervisor de Inversión Privada en Telecomunicaciones, en el marco de sus funciones, adecúa las condiciones de verificación de identidad para duplicados, reposiciones, portabilidad y cambios de titularidad de líneas móviles, incluida la verificación biométrica o mediante identidad digital y la notificación inmediata al titular por un canal alterno.

III. Análisis costo-beneficio

No genera gasto adicional directo: la persecución se realiza con los recursos del Ministerio Público, la Policía Nacional y el Poder Judicial, que ya investigan estas conductas bajo tipos genéricos. El beneficio es la seguridad jurídica: tipos específicos y coherentes con el Código Penal reducen archivamientos por atipicidad, evitan que el ransomware reciba una pena menor que la extorsión común y facilitan la cooperación internacional. Se evita la doble agravación por uso de inteligencia artificial, ya cubierta por la Ley 32314, y se excluye expresamente la investigación de seguridad de buena fe. El incremento de penas por sí solo no garantiza disuasión; la eficacia depende de la capacidad forense del Ministerio Público y la Policía, que no se presupuesta en esta ley.

Normas que modifica

- Ley 30096, Ley de Delitos Informáticos, art. 4-A — *incorpora*
- Ley 30096, Ley de Delitos Informáticos (art. incorporado por Ley 32451), art. 9-A — *modifica*
- Ley 30096, Ley de Delitos Informáticos, art. 11, num. 6 — *incorpora*
- Código Penal, Decreto Legislativo 635, art. 176-C (último párrafo) — *incorpora*
- Código Penal, arts. 200 y 200-A, concordancia de penas — *complementa*
- Resolución Legislativa 30913, Convenio de Budapest, arts. 16 y 35 — *complementa*

Entidades implicadas (quién hace qué)

- **MP** (ejecutora): Ejerce la acción penal, actúa como punto de contacto 24/7 y requiere la conservación rápida de datos (art. 7); adecúa protocolos y publica estadística (DCF Primera y Segunda).
- **PNP** (ejecutora): Investiga y puede requerir conservación rápida (art. 7); adecúa protocolos (DCF Primera).
- **PJ** (supervisora): Autoriza el acceso a datos conservados y su prórroga (art. 7.1 y 7.2) y ordena el decomiso de activos virtuales (art. 6).
- **OSIPTEL** (reguladora): Adecúa la verificación de identidad en duplicados y portabilidad (DCF Tercera).
- **Operadoras** (regulada): Conservan datos a requerimiento con reserva (art. 7) y aplican la verificación reforzada (DCF Tercera).

Sujetos obligados: Toda persona (destinatarios de los tipos penales); proveedores de servicios de telecomunicaciones y digitales respecto de la conservación rápida de datos.

Beneficiarios: Víctimas de ransomware, toma de líneas y chantaje sexual; según El Peruano (2-9-2026), el Ministerio Público registró 29 118 denuncias por delitos informáticos entre enero y julio de 2026.

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

Tipo: neutro

Costo para el Estado: S/ 0 (sin gasto directo)

Horizonte: anual

Financiamiento: Presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Supuestos: La ley no crea órganos ni plazas; la persecución se realiza con los recursos existentes del MP, la PNP y el PJ. No se cuantifica el costo de fortalecer la capacidad forense, que no es exigido por la ley.

Beneficio para el Estado: Menos archivamientos por atipicidad y mejor cooperación internacional; recuperación de activos virtuales para reparación. No cuantificable con información pública.

Beneficio para la sociedad: Mayor protección frente a ransomware, toma de líneas y chantaje sexual con material sintético; certeza jurídica para investigadores de seguridad de buena fe. No cuantificable con información pública.

Inversión privada: No aplica.

Costo para privados: Operadoras: costo marginal de verificación reforzada de identidad en duplicados y portabilidad (DCF Tercera), no cuantificable con información pública.

Riesgos: Sobrecriminalización si los tipos se interpretan extensivamente; dependencia de la capacidad forense; riesgo de concurso aparente si no se verifica el texto vigente del art. 176-C y del art. 200 antes del dictamen.

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

- **Constitucional** — Observaciones graves: La tipificación específica de ciberdelitos es legítima, pero la propuesta tiene problemas de legalidad penal y técnica: el numeral 5 del art. 11 de la Ley 30096 ya fue incorporado por la Ley 32314 (uso de IA), el tipo de 'extorsión informática' tiene pena menor que la extorsión común (art. 200 CP), con lo que privilegia al extorsionador digital, y la sextorsión se superpone con el chantaje sexual ya tipificado. La preservación de datos debe sujetarse a orden judicial para el acceso (art. 2.10).
- **Técnica legislativa** — Observaciones graves: Tipificar el ransomware y el SIM swapping es pertinente, pero el proyecto incorpora un «numeral 5» al art. 11 de la Ley 30096 que ya existe (lo incorporó la Ley 32314), fija para la extorsión informática una pena menor que la de la extorsión común (art. 200 del Código Penal), lo que crea un privilegio injustificado, y se superpone con el chantaje sexual del art. 176-C. Además, usa fórmulas modificatorias incorrectas.
- **Concordancia normativa** — Observaciones graves: Omite dos leyes vigentes que modificaron la Ley 30096: la Ley 32314 (2025), que YA incorporó el numeral 5 del artículo 11 (agravante por uso de IA), y la Ley 32451 (2025), que incorporó el artículo 9-A (activación ilegal de SIM/líneas móviles). El art. 6 colisiona con numeración ocupada, el art. 8-A se superpone con el 9-A y la extorsión informática se pena por debajo de la extorsión común (art. 200 CP).
- **Seguridad** — Observaciones graves: Tipos necesarios, pero con defectos graves: el numeral 5 que se incorpora al art. 11 de la Ley 30096 ya existe (lo incorporó la Ley 32314), la extorsión informática tiene pena básica inferior a la extorsión común del art. 200 del Código Penal (lo que privilegia el ransomware por especialidad), y su redacción ('ventaja de cualquier otra índole' para 'abstenerse de divulgar') puede alcanzar al investigador que fija un plazo de divulgación coordinada.
- **Derecho tecnológico** — Observaciones graves: La modernización de tipos (ransomware, SIM swapping) es pertinente, pero la propuesta colisiona con normas vigentes: la Ley 32314 ya incorporó el numeral 5 del art. 11 de la Ley 30096 (agravante por uso de IA) y el art. 196-A.7 del Código Penal (fraude con voz o imagen manipulada por IA); el nuevo tipo de extorsión informática tendría pena menor que la extorsión común del art. 200 del Código Penal, y la sextorsión se superpone con el chantaje sexual del art. 176-C.

IV. Efecto de la vigencia de la norma

Incorpora el artículo 4-A, modifica el artículo 9-A (incorporado por la Ley 32451) e incorpora el numeral 6 del artículo 11 (el numeral 5 fue incorporado por la Ley 32314) de la Ley 30096; incorpora un párrafo al artículo 176-C del Código Penal. Se concuerda con los artículos 200 y 200-A del Código Penal (el 4-A no fija pena menor que la extorsión común y cede ante el delito más grave), con el artículo 12 de la Ley 30096 (exención por pruebas autorizadas), con el Decreto Legislativo 1182 y con el Convenio de Budapest (Resolución Legislativa 30913). Antes del dictamen debe verificarse en SPIJ el texto vigente de los artículos 9-A, 11 y 176-C y de los artículos 200 y 200-A del Código Penal. No requiere votación de ley orgánica.

V. Indicador de éxito al 2031

A 2031, boletín del Ministerio Público con desagregación de los nuevos tipos y aumento sostenido de la proporción de denuncias por ciberdelitos que llegan a acusación.

Normas relacionadas

- Ley 30096, Ley de Delitos Informáticos (2013) — <https://leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf>
- Ley 30096, texto consolidado (Archivo Digital de la Legislación del Congreso) — https://leyes.congreso.gob.pe/Documentos/ExpVirPal/Texto_Consolidado/30096-TXM.pdf
- Ley 32314, que modifica el Código Penal y la Ley 30096 para incluir el uso de la inteligencia artificial en la comisión de delitos (2025) — https://leyes.congreso.gob.pe/Documentos/2021_2026/ADLP/Texto_Consolidado/32314-TXM.pdf
- Ley 32451, que incorpora el artículo 9-A a la Ley 30096 (activación ilegal de SIM o líneas móviles) (2025) — <https://busquedas.elperuano.pe/dispositivo/NL/2443471-1>
- Decreto Legislativo 1700, que incorpora a la Ley 30096 el delito de adquisición, posesión y tráfico ilícito de datos informáticos (artículo 12-A) — <https://busquedas.elperuano.pe/dispositivo/NL/2480387-2>
- Resolución Legislativa 30913, que aprueba el Convenio sobre la Ciberdelincuencia (Budapest) — <https://busquedas.elperuano.pe/dispositivo/NL/1740637-2>

Antecedentes

Leyes 32314 (2025, inteligencia artificial como agravante) y 32451 (2025, origen PL 09136/2024-CR, activación ilegal de SIM). Proyectos del periodo 2021-2026 (según verificación en SPLEY del revisor normativo): PL 10756/2024-CR, uso indebido de IA en delitos; PL 14045/2025-CR y PL 13035/2025-CR, responsabilidad de personas jurídicas por delitos informáticos (en comisión). Periodo 2026-2031: Proposición 0098-2026-2031-CD de delegación de facultades (en trámite).

Referencias internacionales

- Chile: Ley 21.459, establece normas sobre delitos informáticos (adecuación al Convenio de Budapest) — <https://www.bcn.cl/leychile/navegar?idNorma=1177743>
- Brasil: Lei 14.155/2021 (agrava fraude electrónico e invasión de dispositivo informático) — https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm
- Colombia: Ley 1273 de 2009, de la protección de la información y de los datos — <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>

Fuentes

- El Peruano (02-09-2026): Ciberdelitos más denunciados en el Perú — denuncias ene-jul 2026 según el Ministerio Público — <https://elperuano.pe/noticia/303867-ciberdelitos-mas-denunciados-en-el-peru>
- Ley 32314 (texto consolidado del Congreso) — https://leyes.congreso.gob.pe/Documentos/2021_2026/ADLP/Texto_Consolidado/32314-TXM.pdf
- Congreso de la República: Ley 32451 castiga activación ilegal de líneas móviles y chips falsos — <https://comunicaciones.congreso.gob.pe/noticias/ley-n-32451-castiga-activacion-ilegal-de-lineas-moviles-y-chips-falsos/>

- CiberLATAM: Perú delega facultades sobre ciberdelincuencia (Proposición 0098-2026-2031-CD) — <https://ciberlatam.com/noticias/peru-delega-facultades-ciberdelincuencia>

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/CIB-04.html>