

Ley que fortalece la protección frente a la violencia facilitada por las tecnologías digitales contra las mujeres y los integrantes del grupo familiar, complementando la Ley 30364

Eleva a rango de ley el reconocimiento de la violencia facilitada por tecnologías digitales y, como disposiciones complementarias de la Ley 30364, incorpora medidas de protección digitales (retiro y desindexación de contenido íntimo o sintético, cese de acceso a cuentas, prohibición de geolocalización y software espía) notificadas con firma digital al punto único de contacto, fija plazos de cumplimiento y multas compulsivas a las plataformas, ordena la conservación de evidencia a pedido fiscal y la custodia cifrada del contenido íntimo, sin crear nuevos delitos ni debilitar el cifrado.

Comisión (Cámara de Diputados): Inclusión Social, Familia, Mujer y Pueblos Andinos, Amazónicos y Afroperuanos (+ 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: La Familia, Orden Público y Seguridad, Perú en La Era Digital

I. Exposición de motivos

El Decreto Supremo 002-2025-MIMP modificó el Reglamento de la Ley 30364 para incorporar la «violencia facilitada por las tecnologías digitales», definida como la conducta «cometida, asistida o agravada, en parte o en su totalidad, por el uso de las tecnologías digitales». Sin embargo, ese reconocimiento tiene rango reglamentario y la Ley 30364 no contiene medidas de protección específicamente digitales: su catálogo prevé la prohibición de comunicación «vía chat, redes sociales» u otras formas, pero no órdenes de retiro o desindexación de contenido íntimo difundido sin consentimiento, de cese de acceso a cuentas de la víctima, de prohibición de geolocalización o de instalación de software espía, ni plazos para que las plataformas cumplan. En el plano penal ya existen tipos aplicables (difusión de imágenes con contenido sexual, acoso, chantaje sexual) y la Ley 32314 agravó los delitos cometidos con IA, por lo que esta propuesta no crea delitos; la sextorsión se aborda en CIB-04. Proyectos para incorporar la violencia digital en el artículo 8 de la Ley 30364 (02881/2022-CR, 08350/2023-CR) obtuvieron dictamen en el periodo anterior pero no se aprobaron. La difusión de contenido íntimo se propaga en horas; sin plazos de cumplimiento ni preservación de evidencia, la tutela judicial llega tarde. Además, el Estado mismo puede convertirse en punto de nueva filtración: no existen reglas legales sobre extracción limitada del teléfono de la víctima, custodia cifrada y destrucción del contenido íntimo entregado como evidencia. La Ley 30364 cuenta con un Texto Único Ordenado (D.S. 004-2020-MIMP), pero el Congreso sigue modificando la ley base (p. ej., Ley 31715, que modificó su art. 22 y ordenó adecuar el TUO); como la letra 22-C es materia del PL 02943/2022-CR y no se pudo cotejar el texto consolidado vigente, esta propuesta regula las medidas digitales como disposiciones autónomas complementarias y encarga actualizar el TUO.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE FORTALECE LA PROTECCIÓN FRENTE A LA VIOLENCIA FACILITADA POR LAS TECNOLOGÍAS DIGITALES CONTRA LAS MUJERES Y LOS INTEGRANTES DEL GRUPO FAMILIAR, COMPLEMENTANDO LA LEY 30364

Artículo 1. Objeto

La presente ley tiene por objeto fortalecer la protección frente a la violencia facilitada por las tecnologías digitales contra las mujeres y los integrantes del grupo familiar, mediante disposiciones complementarias de la Ley 30364, Ley para prevenir, sancionar y erradicar la violencia contra las mujeres y los integrantes del grupo familiar.

Artículo 2. Violencia facilitada por tecnologías digitales

Para efectos de la Ley 30364, los tipos de violencia previstos en su artículo 8 comprenden las conductas cometidas, asistidas o agravadas, en todo o en parte, mediante el uso de tecnologías digitales, tales como la

difusión no consentida de contenido íntimo real o generado artificialmente, el acoso u hostigamiento en línea, la suplantación de identidad, la vigilancia o geolocalización no consentida y el control de dispositivos o cuentas.

Artículo 3. Medidas de protección en entornos digitales

3.1 Además de las medidas previstas en el artículo 22 de la Ley 30364, el juzgado puede dictar, entre otras, las siguientes medidas de protección en entornos digitales:

- a) Retiro o inhabilitación del acceso, por la persona agresora y por los proveedores de servicios digitales, del contenido íntimo o sexual, real o generado artificialmente, difundido sin consentimiento de la víctima, y su desindexación en motores de búsqueda.
- b) Prohibición de crear o utilizar perfiles, cuentas o identidades que suplanten a la víctima, y de utilizar cualquier cuenta para contactarla, hostigarla, amenazarla o difundir sus datos personales o contenido íntimo.
- c) Cese inmediato de todo acceso de la persona agresora a las cuentas y dispositivos de la víctima, para lo cual los proveedores, a solicitud de la víctima, cierran las sesiones activas, desvinculan dispositivos y aplicaciones de terceros y eliminan los métodos de recuperación o de segundo factor asociados a la persona agresora.
- d) Prohibición de geolocalizar a la víctima y de instalar o mantener programas o dispositivos de vigilancia en sus bienes.
- e) Orden de conservación de los datos y del contenido necesarios como evidencia, dirigida a los proveedores de servicios digitales.

3.2 La medida identifica con precisión el contenido o la cuenta y se notifica electrónicamente a los proveedores con firma digital del órgano jurisdiccional, a través del canal previsto en el numeral 4.2; el proveedor puede verificar su autenticidad en línea antes de ejecutarla.

3.3 Respecto de servicios de comunicación interpersonal cifrados de extremo a extremo, las medidas se cumplen mediante la suspensión o cancelación de la cuenta de la persona agresora, el retiro del contenido en canales o grupos de acceso abierto y la conservación de los datos disponibles, sin que pueda exigirse el acceso al contenido cifrado ni la alteración del cifrado.

3.4 El proveedor o el tercero que publicó el contenido pueden formular oposición ante el mismo juzgado dentro de los cinco días hábiles de notificados, sin efecto suspensivo cuando se trate de contenido íntimo o sexual. Las medidas no alcanzan la información periodística de interés público que no reproduzca contenido íntimo ni datos que permitan ubicar a la víctima.

Artículo 4. Plazos de cumplimiento para los proveedores de servicios digitales

4.1 Los proveedores de servicios digitales que presten servicios en el territorio nacional cumplen las medidas del artículo 3 en un plazo máximo de veinticuatro horas cuando se trate de contenido íntimo o sexual, y de cuarenta y ocho horas en los demás casos, contadas desde la notificación.

4.2 Las notificaciones judiciales y fiscales se dirigen al punto único de contacto que los proveedores designan conforme a la ley de transparencia de plataformas digitales o, en su defecto, al canal electrónico en español que comuniquen al Poder Judicial y al Ministerio Público.

4.3 Ante el incumplimiento injustificado, el juzgado puede imponer al proveedor multas compulsivas y progresivas conforme al artículo 53 del Código Procesal Civil, de aplicación supletoria, y pone el hecho en conocimiento del Ministerio Público para la determinación de la responsabilidad de los representantes conforme al artículo 368 del Código Penal. Respecto de la persona agresora rige el artículo 24 de la Ley 30364.

Artículo 5. Canal de reporte para víctimas

5.1 Los proveedores de plataformas en línea que alojen contenido de usuarios ponen a disposición de las víctimas un canal de reporte en español, gratuito y prioritario, que puede ser el mismo canal prioritario previsto para la protección de niñas, niños y adolescentes en la ley de la materia, para solicitar el retiro de contenido íntimo o sexual, real o generado artificialmente, difundido sin su consentimiento, aun sin orden judicial. El proveedor verifica de forma razonable que el solicitante es la persona representada o su representante, resuelve con revisión humana en un plazo máximo de cuarenta y ocho horas e informa al usuario que publicó el contenido, quien puede pedir la revisión de la decisión. La presentación de solicitudes a sabiendas falsas genera responsabilidad conforme a ley.

5.2 Los proveedores pueden emplear tecnologías de coincidencia de huellas digitales de contenido para impedir la nueva difusión del contenido retirado, con garantías de protección de datos personales. La huella se genera, siempre que sea técnicamente posible, en el dispositivo de la víctima o por el servicio de atención del

Estado, sin que el contenido se transmita ni se almacene; las plataformas solo reciben y conservan la huella.

Artículo 6. Preservación de evidencia digital

6.1 El Ministerio Público, de oficio o a solicitud de la Policía Nacional del Perú, desde la recepción de la denuncia, puede requerir a los proveedores de servicios digitales la conservación inmediata de los datos informáticos y del contenido relacionados con los hechos, por un plazo de noventa días prorrogable, conforme al Decreto Legislativo 1182, al artículo 16 del Convenio sobre la Ciberdelincuencia y al Código Procesal Penal. La conservación no implica la entrega de los datos; el acceso al contenido de las comunicaciones y a los datos de tráfico requiere mandato judicial motivado conforme al numeral 10 del artículo 2 de la Constitución.

6.2 La recepción de la denuncia no puede condicionarse a que la víctima entregue copias impresas del contenido; basta su identificación mediante enlaces, capturas o descripción.

6.3 La Policía Nacional del Perú y el Ministerio Público: a) limitan la extracción de datos del dispositivo de la víctima a lo pertinente al hecho, con su consentimiento informado, y lo devuelven en el plazo más breve; b) preservan la evidencia con huella criptográfica y registro de cadena de custodia; c) custodian el contenido íntimo en almacenamiento cifrado, con acceso restringido al personal a cargo del caso y bitácora de accesos; d) no incorporan copias del contenido íntimo a expedientes accesibles a terceros, salvo resolución judicial, y prefieren su descripción o huella; y e) destruyen las copias al concluir el proceso, salvo mandato judicial. La difusión del contenido por quien lo custodia se comunica al Ministerio Público para el ejercicio de la acción penal.

Artículo 7. Atención especializada

El Ministerio de la Mujer y Poblaciones Vulnerables incorpora en los servicios de atención existentes de su ámbito la orientación especializada sobre violencia facilitada por tecnologías digitales, incluida la asistencia para el reporte, la preservación de evidencia y la detección y retiro de programas de vigilancia, así como el aseguramiento de cuentas y dispositivos sin destruir evidencia, con cargo a su presupuesto institucional.

Artículo 8. Registro y estadística

Los registros administrativos del Sistema Nacional para la Prevención, Sanción y Erradicación de la Violencia contra las Mujeres y los Integrantes del Grupo Familiar identifican los casos de violencia facilitada por tecnologías digitales, para fines estadísticos y de política pública, con datos anonimizados en su publicación.

Artículo 9. Garantías

Las medidas previstas en la presente ley se dictan por resolución motivada, se limitan al contenido o cuenta identificados y no autorizan el bloqueo general de servicios, la supervisión general de contenidos ni la obligación de debilitar el cifrado de las comunicaciones.

Primera. Disposición Complementaria Final

Adecuación reglamentaria y del Texto Único Ordenado. El Poder Ejecutivo, mediante decreto supremo refrendado por la Ministra o el Ministro de la Mujer y Poblaciones Vulnerables, adecua en un plazo de sesenta días hábiles el Reglamento de la Ley 30364, aprobado por el Decreto Supremo 009-2016-MIMP, y el Texto Único Ordenado de la Ley 30364, aprobado por el Decreto Supremo 004-2020-MIMP, incorporando las disposiciones de los artículos 2 y 3 de la presente ley. El Poder Judicial y el Ministerio Público adecuan sus protocolos en el mismo plazo, en el marco de su autonomía, incluida la notificación con firma digital y la custodia cifrada de evidencia.

Segunda. Disposición Complementaria Final

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

III. Análisis costo-beneficio

La ley no crea delitos, entidades ni plazas: dota a los jueces de medidas de protección adecuadas al entorno digital, fija plazos y apremios a los proveedores y ordena la conservación y custodia segura de evidencia. Los costos para el Estado son de adecuación de protocolos, notificación con firma digital (infraestructura existente del Poder Judicial), custodia cifrada con bitácora sobre la infraestructura existente de la PNP y el Ministerio

Público, y capacitación, absorbibles en sus presupuestos. Para los proveedores, el costo es atender órdenes y reportes en plazos cortos y ejecutar medidas de cuenta (cierre de sesiones, desvinculación), funciones que los grandes servicios ya tienen. El beneficio principal es reducir el daño de la difusión de contenido íntimo y del control digital, evitar la revictimización por filtraciones institucionales y mejorar la persecución penal.

Normas que modifica

- Ley 30364, arts. 8 y 22 (complementa mediante disposiciones autónomas) — *complementa*
- TUO de la Ley 30364, D.S. 004-2020-MIMP, adecuación por el Poder Ejecutivo (DCF Primera) — *complementa*
- Reglamento de la Ley 30364 (modificado por D.S. 002-2025-MIMP), art. 8 — *eleva_rango*
- Decreto Legislativo 1182, conservación de datos (art. 6.1) — *complementa*
- Ley 30096 y Ley 32314, tipos penales vigentes — *complementa*

Entidades implicadas (quién hace qué)

- **PJ** (ejecutora): Dictan las medidas del art. 3, las notifican con firma digital al punto único de contacto, resuelven oposiciones e imponen multas compulsivas (arts. 3 y 4.3).
- **MP** (ejecutora): Requiere la conservación de evidencia de oficio o a pedido de la PNP, custodia cifrada del contenido íntimo (art. 6) y persigue el incumplimiento (art. 4.3).
- **PNP** (ejecutora): Recibe denuncias sin exigir copias impresas, solicita al fiscal la conservación y aplica extracción limitada, cadena de custodia y destrucción de copias (art. 6).
- **MIMP** (rectora): Adecua reglamento y TUO (DCF Primera), incorpora orientación especializada incluida la detección de software espía (art. 7) y los registros (art. 8).
- — (regulada): Cumplen medidas en 24/48 h sin debilitar cifrado, reciben notificaciones en el punto único de contacto y ofrecen reporte prioritario verificado en 48 h (arts. 3 a 5).

Sujetos obligados: Personas agresoras sujetas a medidas; proveedores de servicios digitales que presten servicios en el país; entidades del Sistema Nacional de la Ley 30364.

Beneficiarios: Mujeres e integrantes del grupo familiar víctimas de violencia facilitada por tecnologías digitales. Sin cifra oficial verificada de casos de violencia digital.

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

Tipo: neutro

Costo para el Estado: S/ 0,3–1 millón (único, capacitación y protocolos)

Horizonte: único

Financiamiento: Presupuestos institucionales del PJ, MP, MININTER y MIMP, sin demandar recursos adicionales al Tesoro.

Supuestos: Estimación del editor, no dato oficial. Capacitación virtual de jueces de familia, fiscales, policías y personal de servicios del MIMP mediante plataformas existentes; adecuación de formularios, notificación con firma digital y almacenamiento cifrado con bitácora sobre infraestructura existente de PJ, MP y PNP. Sin plazas nuevas.

Beneficio para el Estado: Mejor calidad probatoria y mayor eficacia de las medidas de protección. No cuantificable.

Beneficio para la sociedad: Reducción del daño a víctimas por retiro oportuno de contenido y cese del control digital. No cuantificable con información pública.

Inversión privada: No aplica.

Costo para privados: Moderado para plataformas (atención en plazos cortos y canal prioritario), bajo si ya operan sistemas equivalentes.

Riesgos: Incumplimiento de proveedores sin domicilio en el país (mitigado por punto único de contacto y multas compulsivas); uso abusivo de reportes para retirar contenido lícito (mitigado por verificación, revisión humana, oposición y exclusión periodística); órdenes falsificadas (mitigado por firma digital); filtración de evidencia custodiada (mitigado por el art. 6.3); limitaciones técnicas en servicios cifrados (art. 3.3).

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

- **Constitucional** — Con observaciones: Las medidas son judiciales, motivadas, específicas y posteriores a la difusión, por lo que no constituyen censura previa (art. 2.4) y cumplen el deber estatal de debida diligencia frente a la violencia de género (Convención de Belém do Pará). Deben ajustarse la prohibición de crear perfiles que 'refieran' a la víctima, que es una restricción anticipada de expresión demasiado amplia; el derecho de defensa de los proveedores y de los terceros alcanzados por la orden; y la separación entre la conservación y el acceso a datos de comunicaciones (art. 2.10).
- **Técnica legislativa** — Con observaciones: Medidas pertinentes, con garantías contra el bloqueo general. Sin embargo, la numeración 22-D salta una letra si el 22-C no existe en la ley vigente. El apercibimiento a los proveedores se apoya en el artículo 24 de la Ley 30364, previsto para la persona agresora, y la conservación de datos a pedido directo de la PNP debe canalizarse por el fiscal.
- **Concordancia normativa** — Con observaciones: No hay ley que modifique la Ley 30364 para la violencia digital (el D.S. 002-2025-MIMP, del 4-abr-2025, la incorporó solo en el reglamento; luego lo modificó el D.S. 004-2025-MIMP). La propuesta no crea delitos y remite la sextorsión a CIB-04: correcto. Observaciones: numeración (22-C es materia del PL 02943/2022-CR con dictamen; existe TUO de la Ley 30364), punto de contacto duplicado con DER-03/IA-07 y base de la preservación de evidencia.
- **Seguridad** — Observaciones graves: Avance importante (medidas digitales, preservación de evidencia, huellas de contenido), pero la ley ignora la custodia del contenido íntimo que la víctima entrega a la PNP y al Ministerio Público: sin reglas de acceso restringido, cifrado, extracción limitada del dispositivo y destrucción, el propio Estado puede convertirse en punto de nueva filtración. Faltan además garantías de cadena de custodia y la autenticación de las órdenes que se notifican electrónicamente a los proveedores.
- **Derecho tecnológico** — Con observaciones: Medidas pertinentes y realistas: 24 h para contenido íntimo es más exigente que las 48 h del TAKE IT DOWN Act (EE. UU., 2025) y la conservación de 90 días prorrogables coincide con el art. 16 del Convenio de Budapest, del que el Perú es parte. Requiere ajustes técnicos: las órdenes de retiro no pueden ejecutarse sobre mensajería cifrada de extremo a extremo, el canal de reporte sin orden judicial necesita verificación y protección contra solicitudes abusivas, y las medidas sobre cuentas deben describirse en términos ejecutables (cierre de sesiones, desvinculación de dispositivos).

IV. Efecto de la vigencia de la norma

Complementa la Ley 30364 (arts. 8, 22 y 24) mediante disposiciones autónomas, sin incorporar articulado con letra (22-C es materia del PL 02943/2022-CR y la numeración vigente no pudo cotejarse en el texto consolidado); el Poder Ejecutivo las incorpora al TUO aprobado por D.S. 004-2020-MIMP, como ocurrió con la Ley 31715. Eleva a rango de ley el reconocimiento del D.S. 002-2025-MIMP (reglamento modificado luego por el D.S. 004-2025-MIMP, según el revisor normativo). Se concuerda con el D. Leg. 1182 y el art. 16 del Convenio sobre la Ciberdelincuencia (conservación de datos), el Código Procesal Civil (art. 53, supletorio), el Código Penal (art. 368), la Ley 30096, la Ley 32314 y la Ley 31664; la tipificación de la sextorsión corresponde a CIB-04. No deroga normas.

V. Indicador de éxito al 2031

Al 2028, reglamento, TUO y protocolos adecuados (incluida notificación con firma digital y custodia cifrada) y casos de violencia digital identificados en los registros del Sistema Nacional; al 2031, tiempo de cumplimiento de las medidas del art. 3 por los proveedores medido y publicado, sin incidentes de filtración de evidencia íntima custodiada por el Estado.

Normas relacionadas

- Ley 30364, Ley para prevenir, sancionar y erradicar la violencia contra las mujeres y los integrantes del grupo familiar (arts. 8, 22 y 24) — https://leyes.congreso.gob.pe/Documentos/ExpVirPal/Texto_Consolidado/30364-TXM.pdf
- Decreto Supremo 002-2025-MIMP, que modifica el Reglamento de la Ley 30364 (violencia facilitada por las tecnologías digitales) — <https://busquedas.elperuano.pe/dispositivo/NL/2387420-5>
- Ley 32314, que modifica el Código Penal y la Ley 30096 para incluir el uso de la IA en la comisión de delitos — https://leyes.congreso.gob.pe/Documentos/2021_2026/ADLP/Texto_Consolidado/32314-TXM.pdf

- Ley 30096, Ley de Delitos Informáticos, texto consolidado — https://leyes.congreso.gob.pe/Documentos/ExpVirPal/Texto_Consolidado/30096-TXM.pdf
- Ley 31715, que modifica la Ley 30364 (arts. 15, 16, 22, 23-A y 45) y ordena adecuar su TUO (D.S. 004-2020-MIMP) — https://leyes.congreso.gob.pe/Documentos/2021_2026/ADLP/Texto_Consolidado/31715-TXM.pdf
- Ley 31664, que modifica la Ley 30254 (uso seguro de TIC por niñas, niños y adolescentes) — https://leyes.congreso.gob.pe/Documentos/2021_2026/ADLP/Texto_Consolidado/31664-TXM.pdf
- Decreto Legislativo 1182 (uso de datos de geolocalización y conservación de datos de telecomunicaciones; El Peruano, 27-jul-2015) — <https://www.leyes.congreso.gob.pe/Documentos/DecretosLegislativos/01182.pdf>

Antecedentes

Relacionados (SPLEY, data/antecedentes.json): 02881/2022-CR (incorpora la violencia digital al art. 8 de la Ley 30364, con dictamen); 08350/2023-CR (ciberacoso como tipo de violencia, con dictamen); 09717/2024-CR (denuncias por canales digitales, en comisión); 02943/2022-CR (art. 22-C, notificación electrónica de medidas de protección, con dictamen); 04274/2022-CR (vigilancia electrónica personal en la Ley 30364, con dictamen); 05222/2022-CR (delitos de acoso y difusión de imágenes, con dictamen); 10308/2024-CR (violencia digital contra menores, en comisión); 00006-2026-2031-CD (violencia sexual digital mediante IA, en comisión); 00447-2026-2031-CD (retiro urgente de contenido digital para proteger a niños y adolescentes, en comisión); 00367-2026-2031-CD (ciberacoso escolar, Ley 29719, en comisión).

Referencias internacionales

- Reino Unido: Online Safety Act 2023 (deberes de los proveedores y delitos de difusión de imágenes íntimas) — <https://www.legislation.gov.uk/ukpga/2023/50/contents>
- Unión Europea: Reglamento (UE) 2022/2065, Ley de Servicios Digitales (art. 9, órdenes de actuación contra contenidos ilícitos) — <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

Fuentes

- El Peruano: D.S. 002-2025-MIMP (4-abr-2025) — <https://busquedas.elperuano.pe/dispositivo/NL/2387420-5>
- Ley 30364, texto consolidado (Archivo Digital de la Legislación del Congreso) — https://leyes.congreso.gob.pe/Documentos/ExpVirPal/Texto_Consolidado/30364-TXM.pdf
- Ley 32314, texto consolidado (Congreso) — https://leyes.congreso.gob.pe/Documentos/2021_2026/ADLP/Texto_Consolidado/32314-TXM.pdf

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/DER-07.html>