

Ley que establece requisitos mínimos de ciberseguridad para dispositivos conectados de consumo

Establece los requisitos mínimos de ciberseguridad para dispositivos conectados de consumo (sin contraseñas por defecto universales, actualizaciones de seguridad, política de gestión de vulnerabilidades y periodo de soporte informado), que se desarrollan mediante reglamento técnico conforme a la Ley 30224 y a los compromisos OMC y CAN; integra la declaración de conformidad a la homologación del MTC, incluye los equipos que los operadores entregan a sus abonados y tipifica el incumplimiento como infracción al Código de Protección y Defensa del Consumidor.

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:** media · **Costo fiscal:** bajo · **Plazo:** mediano
Plan Perú 2050: Ciber Seguridad, Ciudades Inteligentes, Industria

I. Exposición de motivos

Cámaras de vigilancia, enrutadores domésticos, televisores, cerraduras y otros dispositivos conectados se comercializan en el Perú sin requisitos legales de ciberseguridad. Los dispositivos con contraseñas por defecto idénticas o sin actualizaciones son reclutados en redes de bots que lanzan ataques de denegación de servicio contra entidades y empresas, y pueden exponer la intimidad de los hogares. Entre ellos están los enrutadores y decodificadores que los operadores entregan en comodato. El Código de Protección y Defensa del Consumidor exige idoneidad e información, pero no define estándares de seguridad digital, y el consumidor no sabe cuántos años recibirá parches un equipo. Los equipos que usan el espectro ya requieren homologación del MTC, pero esta no evalúa ciberseguridad. El Reino Unido (PSTI Act 2022, vigente desde 2024) prohibió las contraseñas por defecto universales y obligó a informar el periodo de soporte; la Unión Europea aprobó el Reglamento de Ciberresiliencia (2024) y Estados Unidos creó el sello voluntario Cyber Trust Mark. No hay en el Perú datos oficiales sobre dispositivos vulnerables. Como todo requisito obligatorio de producto, el piso regulatorio debe adoptarse como reglamento técnico, con notificación internacional.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE ESTABLECE REQUISITOS MÍNIMOS DE CIBERSEGURIDAD PARA DISPOSITIVOS CONECTADOS DE CONSUMO

Artículo 1. Objeto

La presente ley tiene por objeto establecer los requisitos mínimos de ciberseguridad de los dispositivos conectados de consumo que se comercializan o entregan a consumidores en el territorio nacional, a fin de proteger a los consumidores y la seguridad de las redes.

Artículo 2. Ámbito

2.1. Se entiende por dispositivo conectado de consumo todo producto destinado a consumidores finales capaz de conectarse a internet o a una red de área local, directa o indirectamente.

2.2. Se incluyen los equipos terminales que los operadores de telecomunicaciones entregan a sus abonados bajo cualquier título; en tal caso, el operador asume las obligaciones del fabricante o importador respecto de la aplicación de actualizaciones de seguridad, bajo la supervisión del Organismo Supervisor de Inversión Privada en Telecomunicaciones.

2.3. Se excluyen los dispositivos médicos regulados por su normativa especial. Los computadores personales, teléfonos móviles y tabletas están excluidos del literal a) del numeral 3.1 del artículo 3 cuando su sistema operativo exija la creación de credenciales en la configuración inicial.

Artículo 3. Requisitos mínimos y reglamento técnico

3.1. El Ministerio de la Producción, en coordinación con el Ministerio de Transportes y Comunicaciones y la Presidencia del Consejo de Ministros, aprueba mediante reglamento técnico, conforme a la Ley 30224, Ley que crea el Sistema Nacional para la Calidad y el Instituto Nacional de Calidad, y a la normativa andina sobre reglamentos técnicos, los requisitos mínimos de ciberseguridad, que comprenden como mínimo:

- a) No utilizar contraseñas por defecto universales ni contraseñas que cumplan los criterios de debilidad que establezca el reglamento técnico.
- b) Contar con un mecanismo para recibir actualizaciones de seguridad.
- c) Estar respaldados por una política pública y accesible de recepción y gestión de vulnerabilidades, que indique un punto de contacto, el plazo de acuse de recibo y de información sobre el estado del reporte, que no condicione la recepción a la renuncia de derechos del informante y que sea compatible con el régimen de divulgación coordinada de vulnerabilidades que establezca la ley.

3.2. El reglamento técnico toma como referencia los estándares internacionales de ciberseguridad para dispositivos de consumo, a fin de permitir el reconocimiento mutuo.

Artículo 4. Periodo de soporte de seguridad

4.1. El fabricante o importador informa, de forma clara, visible y comparable, en el empaque, en la ficha del producto y en los canales de venta en línea, el periodo mínimo durante el cual el dispositivo recibirá actualizaciones de seguridad. Cuando no se declare periodo, se presume que no existe soporte y así se informa al consumidor.

4.2. El incumplimiento del periodo de soporte declarado constituye infracción al deber de idoneidad del artículo 18 de la Ley 29571, Código de Protección y Defensa del Consumidor.

4.3. El deber de información sobre el periodo de soporte de seguridad previsto en este artículo es el único aplicable a esa materia; las normas sobre reparación de aparatos remiten a él.

Artículo 5. Declaración de conformidad y homologación

5.1. El fabricante o importador emite una declaración de conformidad con el reglamento técnico, que conserva a disposición de la autoridad durante el periodo de soporte declarado. Se reconocen las certificaciones emitidas conforme a estándares internacionales equivalentes.

5.2. Para los dispositivos sujetos a homologación de equipos y aparatos de telecomunicaciones, la declaración de conformidad se presenta en el mismo procedimiento de homologación ante el Ministerio de Transportes y Comunicaciones y es requisito para obtenerla.

Artículo 6. Obligaciones de los distribuidores y plataformas

Los distribuidores y las plataformas de comercio electrónico que comercialicen dispositivos conectados verifican que se informe el periodo de soporte y retiran de la venta los productos sobre los que la autoridad haya determinado incumplimiento.

Artículo 7. Fiscalización y sanciones

7.1. El incumplimiento de los artículos 4 a 6 y del reglamento técnico por fabricantes, importadores, distribuidores o plataformas de comercio electrónico constituye infracción a los deberes de información (artículo 2) e idoneidad (artículo 18) de la Ley 29571 y se sanciona por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual conforme a sus artículos 108 y 110, sin perjuicio de la fiscalización del reglamento técnico por la autoridad sectorial competente.

7.2. El OSIPTEL supervisa y sanciona a los operadores respecto de los equipos del numeral 2.2, conforme a la Ley 27336.

7.3. 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, brinda soporte técnico y puede emitir alertas sobre dispositivos con vulnerabilidades críticas no corregidas.

Artículo 8. Contrataciones públicas

Las entidades públicas solo contratan dispositivos conectados que cumplan el reglamento técnico y cuyo periodo de soporte declarado cubra al menos la vida útil prevista del bien, en el marco de la Ley 32069, Ley General de Contrataciones Públicas.

Primera. Disposición Complementaria Final

Reglamentación y reglamento técnico. El Poder Ejecutivo, mediante decreto supremo refrendado por el presidente del Consejo de Ministros, el ministro de la Producción y el ministro de Transportes y Comunicaciones, previa opinión del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, aprueba el reglamento técnico en un plazo no mayor de ciento ochenta días hábiles contados a partir del día siguiente de la publicación de la presente ley. El proyecto se notifica a la Organización Mundial del Comercio y a la Comunidad Andina conforme a los compromisos sobre obstáculos técnicos al comercio, con el plazo de comentarios correspondiente.

Segunda. 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.

Única. Disposición Complementaria Transitoria

Exigibilidad y productos en inventario. Las obligaciones de los artículos 3 a 6 son exigibles a los dieciocho meses de la publicación del reglamento técnico y no alcanzan a los productos ingresados al país con anterioridad a esa fecha.

III. Análisis costo-beneficio

Costo fiscal bajo: Indecopi fiscaliza dentro de sus funciones de protección al consumidor, el MTC integra la verificación en la homologación existente y PRODUCE elabora el reglamento técnico con su personal; el editor estima un costo incremental de S/ 0,5 a 1,5 millones anuales. Los requisitos son mínimos y coinciden con los exigidos en Reino Unido y la Unión Europea, por lo que la mayoría de fabricantes globales ya los cumple; el costo adicional recae en importadores de productos de muy bajo costo sin soporte, y en operadores que deben actualizar los equipos que entregan en comodato. El beneficio es doble: protege la privacidad y seguridad de los hogares y reduce la disponibilidad de dispositivos que alimentan redes de bots contra infraestructuras nacionales. El procedimiento de reglamento técnico con notificación OMC y CAN evita cuestionamientos como obstáculo al comercio.

Normas que modifica

- Ley 29571, Código de Protección y Defensa del Consumidor, arts. 2, 18, 108 y 110 — *complementa*
- Ley 30224, Sistema Nacional para la Calidad, reglamentos técnicos — *complementa*
- TUO de la Ley de Telecomunicaciones (D.S. 013-93-TCC), homologación de equipos — *complementa*
- Ley 32069, Ley General de Contrataciones Públicas, requisito en contrataciones (art. 8 de la ley) — *complementa*

Entidades implicadas (quién hace qué)

- **PRODUCE** (reglamentadora): Aprueba el reglamento técnico de requisitos mínimos (art. 3.1; DCF Primera).
- **MTC** (ejecutora): Integra la declaración de conformidad en la homologación de equipos (art. 5.2).
- **INDECOPI** (sancionadora): Fiscaliza y sanciona a fabricantes, importadores, distribuidores y plataformas (art. 7.1).
- **OSIPTEL** (sancionadora): Supervisa la actualización de equipos entregados por operadores (arts. 2.2 y 7.2).
- **PCM-SGTD / CNSD** (consultiva): Soporte técnico y alertas sobre dispositivos vulnerables (art. 7.3).
- **INACAL / MINCETUR** (consultiva): Normalización y acreditación; notificación OTC a la OMC y la CAN (DCF Primera).

Sujetos obligados: Fabricantes e importadores de dispositivos conectados de consumo; distribuidores y plataformas de comercio electrónico; operadores de telecomunicaciones respecto de los equipos que entregan a sus abonados; entidades públicas como compradoras.

Beneficiarios: Hogares usuarios de dispositivos conectados y, de forma indirecta, entidades y empresas expuestas a ataques de redes de bots. No cuantificable con información pública.

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

Tipo: gasto

Costo para el Estado: S/ 0,5–1,5 millones/año (estimación del editor)

Horizonte: anual, desde 2028

Financiamiento: Presupuesto institucional de PRODUCE, MTC, Indecopi y OSIPTEL sin demandar recursos adicionales al Tesoro Público.

Supuestos: Elaboración del reglamento técnico con personal existente de PRODUCE; 2 a 4 plazas adicionales en Indecopi para vigilancia de mercado y verificación en la homologación del MTC; costo laboral supuesto de S/ 120 000 a S/ 200 000 por plaza y gastos de ensayos de muestras. Supuestos propios, sin fuente oficial.

Beneficio para el Estado: Menos dispositivos disponibles para redes de bots que atacan servicios públicos; compras públicas con soporte asegurado. No cuantificable con información pública.

Beneficio para la sociedad: Protección de la privacidad y seguridad de los hogares e información comparable sobre el soporte de seguridad. No cuantificable con información pública.

Inversión privada: No aplica.

Costo para privados: Bajo para fabricantes globales ya sujetos a PSTI o CRA; mayor para importadores de productos de muy bajo costo sin soporte; costo operativo moderado para operadores que actualizan equipos en comodato.

Riesgos: Demora en la aprobación del reglamento técnico; capacidad limitada de vigilancia de mercado en comercio electrónico transfronterizo; posible alza marginal de precios de dispositivos de gama baja.

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

- **Constitucional** — Con observaciones: Los requisitos mínimos son una restricción proporcional a la libertad de comercio (art. 59) en tutela del consumidor (art. 65). Debe vincularse la infracción al Código de Protección y Defensa del Consumidor para cumplir la tipicidad y respetar el procedimiento de reglamentos técnicos.
- **Técnica legislativa** — Con observaciones: Son requisitos mínimos claros y alineados con los estándares comparados, pero la potestad sancionadora de INDECOPI se invoca de forma genérica sin vincular las nuevas obligaciones al régimen de infracciones del Código, se remite a una «autoridad nacional de ciberseguridad» inexistente y no se prevé la naturaleza de reglamento técnico de la norma de desarrollo.
- **Concordancia normativa** — Con observaciones: No existe norma peruana vigente con requisitos de ciberseguridad para dispositivos conectados de consumo. Pero un requisito obligatorio para comercializar productos es un 'reglamento técnico', sujeto al Sistema Nacional para la Calidad (Ley 30224), a la Decisión 827 de la CAN y al Acuerdo OTC de la OMC; y para equipos de telecomunicaciones ya existe homologación del MTC. Sin ese engarce, la ley sería inaplicable o cuestionable como obstáculo técnico al comercio.
- **Seguridad** — Con observaciones: Requisitos mínimos correctos, proporcionales y equivalentes a los de referencia internacional. La principal brecha es que los equipos terminales instalados por los operadores (routers y decodificadores en comodato), fuente frecuente de redes de bots, pueden quedar fuera al no 'comercializarse' al consumidor.
- **Derecho tecnológico** — Con observaciones: Piso regulatorio mínimo, alineado con PSTI (Reino Unido), CRA (UE) y ETSI EN 303 645; técnicamente correcto. Por ser un reglamento técnico sobre productos, debe notificarse a la OMC (Acuerdo OTC) y a la CAN, y su punto de control más eficaz es la homologación de equipos de telecomunicaciones del MTC, no solo la fiscalización ex post de Indecopi. Debe reemplazar la referencia a una 'autoridad nacional de ciberseguridad' inexistente.

IV. Efecto de la vigencia de la norma

Complementa la Ley 29571 (arts. 2, 18, 108 y 110: tipifica el incumplimiento como infracción de consumo), la Ley 30224 (procedimiento de reglamentos técnicos), la Decisión 827 de la Comunidad Andina y el Acuerdo OTC de la OMC, el TUO de la Ley de Telecomunicaciones (D.S. 013-93-TCC) y su régimen de homologación, la Ley 27336, la Ley 32069 y el Decreto de Urgencia 007-2020. Es la norma de referencia sobre el periodo de soporte de seguridad. No requiere votación de ley orgánica.

V. Indicador de éxito al 2031

A 2030, reglamento técnico vigente y notificado a la OMC y la CAN; 100 % de dispositivos conectados nuevos en venta con periodo de soporte informado; informe anual de fiscalización de Indecopi publicado.

Normas relacionadas

- Ley 29571, Código de Protección y Defensa del Consumidor — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/29571.pdf>
- Ley 30224, Ley que crea el Sistema Nacional para la Calidad y el Instituto Nacional de Calidad — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/30224.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>

Antecedentes

Según verificación en SPLEY del revisor normativo, no se identificaron proyectos del periodo 2021-2026 sobre ciberseguridad de dispositivos conectados de consumo.

Referencias internacionales

- Reino Unido: Product Security and Telecommunications Infrastructure Act 2022 — <https://www.legislation.gov.uk/ukpga/2022/46/contents>
- Reino Unido: PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023 — <https://www.legislation.gov.uk/uksi/2023/1007/contents/made>
- Unión Europea: Reglamento (UE) 2024/2847 de Ciberresiliencia (productos con elementos digitales) — <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>
- Estados Unidos: FCC U.S. Cyber Trust Mark (etiquetado de ciberseguridad de dispositivos IoT) — <https://www.fcc.gov/CyberTrustMark>

Fuentes

- UK legislation: PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023 — <https://www.legislation.gov.uk/uksi/2023/1007/contents/made>
- FCC: U.S. Cyber Trust Mark — <https://www.fcc.gov/CyberTrustMark>
- Apaxi (07-09-2026): Normas de ciberseguridad para empresas en el Perú — <https://apaxi.info/2026/09/07/normas-ciberseguridad-empresas-peru/>

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