

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO

RECIBIDO

RU 2256402

23 MARZO 2026 03:56 p. m.

FIRMADO DIGITALMENTE: ELOPEZ

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

**COMISIÓN DE TRANSPORTES Y COMUNICACIONES
PERÍODO ANUAL DE SESIONES 2025-2026
Segunda Legislatura Ordinaria**

Señor presidente:

Ha ingresado para estudio y dictamen de la Comisión de Transportes y Comunicaciones del Congreso de la República, el Proyecto de Ley 4247/2022-CR, presentado por el congresista Alfredo Pariona Sinche, del grupo parlamentario Bancada Socialista, por el cual se propone la Ley que establece medidas para proteger a la ciudadanía de los riesgos de seguridad digital que originan la sustracción de equipos móviles.

Después del debate correspondiente, la Comisión de Transportes y Comunicaciones, en su decimotercera sesión ordinaria realizada el 16 de marzo de 2026, aprobó por mayoría el presente dictamen.

Votaron a favor los señores congresistas Juan Carlos Mori Celis, Karol Ivett Paredes Fonseca, Segundo Héctor Acuña Peralta, Jorge Luis Flores Ancachi, Alfredo Pariona Sinche, José Bernardo Pazo Nunura, Luis Raúl Picón Quedo, Wilson Quispe Mamani, María Elizabeth Taipe Coronado, Héctor Valer Pinto y Oscar Zea Choquechambi.

Se abstuvieron los señores congresistas María Antonieta Agüero Gutiérrez, Auristela Ana Obando Morgan y Cruz María Zeta Chunga.

Presentaron licencia los señores congresistas Patricia Rosa Chirinos Venegas, Jeny Luz López Morales, Roberto Sánchez Palomino Rosío Torres Salinas y Norma Martina Yarrow Lumbreras.

I. SITUACIÓN PROCESAL

1.1. Admisibilidad de las iniciativas legislativas

La iniciativa legislativa en estudio cumple con los requisitos generales y específicos establecidos en los artículos 75, 76 y 77 del Reglamento del Congreso de la República y su modificatoria según Resolución Legislativa del Congreso 205-2005-CR (publicada el 21 de julio de 2006)¹, para la admisibilidad de los proyectos de ley, por lo que se procedió a solicitar opiniones y a realizar el estudio correspondiente. Asimismo, se ha tomado en consideración para su elaboración el artículo 76 del Reglamento del Congreso, referido a la relación que se tiene con la Agenda Legislativa 2024-2025², aprobada de conformidad con el artículo 29³ y las políticas de Estado expresadas en el

¹

[https://www2.congreso.gob.pe/Sicr/RelatAgenda/proapro.nsf/ProyectosAprobadosPortal/11C84305AF987435052571B0007189CF/\\$FILE/RLC0252005ModificacionReglamento.pdf](https://www2.congreso.gob.pe/Sicr/RelatAgenda/proapro.nsf/ProyectosAprobadosPortal/11C84305AF987435052571B0007189CF/$FILE/RLC0252005ModificacionReglamento.pdf)

² La Agenda Legislativa es un instrumento concertado de planificación del trabajo parlamentario en materia legislativa y que el debate de los proyectos de ley ahí contenidos tiene prioridad, tanto en las comisiones como en el Pleno del Congreso

³ Artículo 29.

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

Acuerdo Nacional. La referida Agenda Legislativa 2024-2025 fue aprobada mediante Resolución Legislativa del Congreso N° 006-2024-2025-CR, la cual, en el Objetivo IV: AFIRMACIÓN DE UN ESTADO EFICIENTE, TRANSPARENTE Y DESCENTRALIZADO, incluye como política de Estado la SOCIEDAD DE LA INFORMACIÓN Y SOCIEDAD DEL CONOCIMIENTO.

1.2. Antecedentes procedimentales

El Proyecto de Ley 4247/2022-CR, fue presentado ante el Área de Trámite Documentario el 14 de febrero de 2023. Fue decretado e ingresó a la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas como primera y única comisión dictaminadora, el 17 de febrero de 2023, para su estudio y dictamen.

Con fecha 14 de diciembre de 2023, la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, aprueba por unanimidad, la inhibición de la Comisión para dictaminar por cuyo objeto principal está relacionado a la Comisión de Transportes y Comunicaciones.

Con fecha 27 de febrero de 2024, el Consejo Directivo, en sesión del 27 de febrero de 2024, atendiendo al análisis sobre el contenido de la materia del proyecto de ley, por parte de la comisión dictaminadora, acordó que pase a la Comisión de Transportes y Comunicaciones.

1.3. Antecedentes parlamentarios

La presente iniciativa legislativa no tiene antecedentes parlamentarios con similar materia en periodos parlamentarios anteriores.

II. CONTENIDO DEL PROYECTO DE LEY

El Proyecto de Ley 4247/2022-CR, busca establecer medidas para proteger a la ciudadanía de los riesgos de seguridad digital que originan la sustracción de equipos móviles y promover la confianza digital en el país. El proyecto consta de cinco artículos, una disposición complementaria final, una disposición complementaria modificatoria y

(...)

Al inicio del Período Anual de Sesiones, los Grupos Parlamentarios y el Consejo de Ministros presentarán una propuesta detallando los temas y proyectos de ley que consideren necesario debatir y aprobar durante dicho periodo. El Pleno del Congreso votará la inclusión en la Agenda Legislativa de estos proyectos, incluyéndose en la misma sólo a los que obtengan mayoría simple. El debate de estos proyectos de ley tiene prioridad, tanto en Comisiones como en el Pleno del Congreso, salvo lo dispuesto por el artículo 105 de la Constitución Política del Estado y no impide que puedan dictaminarse y debatirse otros proyectos.

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

una disposición complementaria derogatoria que deroga el artículo 5 del Decreto Legislativo 1338.

El artículo 1, respecto al objeto de la ley, establece medidas para proteger a la ciudadanía de los riesgos de seguridad digital generados por la sustracción de equipos móviles y promover la confianza digital, y en su artículo 2, dispone medidas sobre el uso de servicios, plataformas y tecnologías digitales para mitigar los riesgos originados por la sustracción de equipos móviles y prevenir el uso de las TIC con fines delictivos.

En el artículo 3, respecto al intercambio de información entre entidades públicas y privadas, se autoriza al Ministerio Público, al Poder Judicial y a la Policía Nacional a acceder a datos de identificación personal mediante mecanismos de interoperabilidad; obliga a entidades públicas y privadas a facilitar dichos datos respetando la normativa sobre datos personales, y el artículo 4, ordena que entidades públicas y organizaciones privadas promuevan el uso de tecnologías y mecanismos de seguridad digital para bloquear dispositivos móviles de forma remota.

Mientras que, en su artículo 5, señala que la implementación de la ley se financia con cargo al presupuesto institucional de las entidades involucradas, y finalmente en su Disposición Modificatoria, propone modificar los artículos 6 y 8 del Decreto Legislativo 1338. El artículo 6 permite al Ministerio Público, a la Policía Nacional y al Poder Judicial acceder al Registro Nacional de Equipos Terminales Móviles (RENTESEG) mediante mecanismos de interoperabilidad. El artículo 8 obliga a las empresas operadoras a verificar la identidad de quien contrata servicios móviles mediante sistemas biométricos o tecnologías que garanticen niveles similares de seguridad. También se deroga el artículo 5 del Decreto Legislativo 1338.

III. MARCO NORMATIVO

3.1. Legislación nacional

- a) **Constitución Política del Perú:** Reconoce el derecho a la intimidad personal y familiar, así como el derecho al secreto de comunicaciones y documentos privados (artículo 2, numerales 6 y 10). Toda injerencia en datos personales debe estar prevista por ley, obedecer a una finalidad legítima y ser proporcional.
- b) **Ley 29733, Ley de Protección de Datos Personales:** Establece el marco para la protección de los datos personales en Perú. Su objeto es garantizar el derecho fundamental a la protección de datos personales y asegurar un tratamiento adecuado de la información. Ordena que el tratamiento de datos requiera consentimiento del titular y la aplicación de medidas de seguridad adecuadas (arts. 2 y 21). La autoridad de protección es la Autoridad Nacional de Protección de Datos Personales (ANPD).

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

- c) **Decreto Legislativo 1412, Ley de Gobierno Digital:** Busca modernizar la administración pública mediante la transformación digital. Sus pilares son la identidad digital, la interoperabilidad y la seguridad digital. El Estado debe garantizar que las entidades compartan datos mediante la Plataforma de Interoperabilidad del Estado Peruano (PIDE) para evitar que los ciudadanos aporten información varias veces. El marco enfatiza que la gobernanza digital requiere gestión de riesgos y cumplimiento de estándares internacionales, y que las entidades públicas deben adoptar medidas de seguridad para proteger los datos. El Decreto Supremo 029-2021-PCM, Reglamento de la Ley de Gobierno Digital, confirma que la PCM (a través de la Secretaría de Gobierno y Transformación Digital) es responsable de la gobernanza y la adopción de tecnologías, y que la interoperabilidad solo puede desarrollarse conforme a la Ley de Protección de Datos Personales.
- d) **Decreto Legislativo 1338, Registro Nacional de Equipos Terminales Móviles (RENTESEG).** Crea un registro de IMEI para equipos móviles y obliga a las empresas operadoras a: (i) Verificar plenamente la identidad de los contratantes mediante verificación biométrica o tecnologías equivalentes y bloquear los equipos reportados como robados; (ii) Bloquear y suspender el servicio a equipos con IMEI inválido o que no estén en la lista blanca, y prohibir la reactivación de equipos incluidos en la lista negra; y (iii) Compartir información con el registro y con listas negras internacionales para impedir el uso de equipos robados, en cumplimiento de la Decisión 786 de la Comunidad Andina.
- e) **Decreto Legislativo 1246, Ley de Simplificación Administrativa.** Obliga a las entidades públicas a intercambiar gratuitamente información y bases de datos mediante interoperabilidad para la tramitación de procedimientos administrativos, y precisa que la información protegida por la Ley 29733 sólo puede compartirse con autorización expresa del titular.
- f) **Código Penal.** Tipifica el robo y el hurto (arts. 186 y 185) y establece agravantes cuando se produce con violencia. También sanciona la receptación de objetos robados (art. 194). La materialización de la propuesta requiere articular con las disposiciones penales vigentes para perseguir a las organizaciones que roban dispositivos.

3.2. Legislación comparada

- a) **Estados Unidos (Minnesota y California):** Minnesota aprobó en 2014 la Ley HF 1952 que exige que todos los smartphones vendidos en el estado incorporen un "kill switch" que permita al usuario borrar la información y desactivar el teléfono robado, con la posibilidad de reversión si es recuperado. California promulgó la Senate Bill 962 que obliga a instalar por defecto una función de desactivación remota resistente a reinstalaciones de software. Según estudios citados en medios,

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

en ciudades como San Francisco el robo de smartphones se redujo 50 % entre 2013 y 2017 tras la entrada en vigor de estas leyes⁴.

- b) Chile:** La ley chilena de 2023 exige que las empresas de telecomunicaciones bloqueen, en un plazo máximo de 24 horas, los celulares robados desde comercios o almacenes y mantengan un registro centralizado. Las empresas deben exigir una denuncia policial y entregar constancia de bloqueo; el objetivo es desincentivar la comercialización de equipos robados. La norma también busca coordinar a operadores y autoridades para prevenir la reventa en mercados informales⁵.
- c) Comunidad Andina – Decisión 786 (2012):** Establece un marco para el intercambio de información sobre equipos terminales móviles perdidos, robados o recuperados entre los países miembros (Bolivia, Colombia, Ecuador y Perú). Su objeto es facilitar el bloqueo de IMEI a nivel regional. La decisión define conceptos como bloqueo, lista negra, EIR (registro de identidad de equipo) y establece que las administraciones deberán compartir información de sus registros nacionales. El Decreto Legislativo 1338 incorpora estas obligaciones en el ordenamiento peruano.

3.3. Normas convencionales

- a) Declaración Universal de Derechos Humanos (artículo 12) y Pacto Internacional de Derechos Civiles y Políticos (artículo 17).** Ambos instrumentos prohíben la injerencia arbitraria en la vida privada y las comunicaciones y exigen que la ley proteja a las personas contra esa injerencia. El Comité de Derechos Humanos y la Corte Interamericana de Derechos Humanos han establecido que cualquier limitación a la privacidad debe pasar un test de legalidad, necesidad y proporcionalidad.
- b) Convención Americana sobre Derechos Humanos (artículo 11).** Reconoce el derecho a la honra y a la vida privada, y exige que se garantice la protección contra intromisiones abusivas. Perú, como Estado parte, debe asegurar que las medidas de seguridad digital respeten este estándar.

⁴ States Evaluating Smartphone 'Kill Switch' Legislation: <https://www.govtech.com/public-safety/states-evaluating-smartphone-kill-switch-legislation.html>

⁵ Celular robado, celular bloqueado: nueva norma obliga a empresas a deshabilitar teléfonos hurtados: <https://www.entnerd.com/celular-robado-celular-bloqueado-nueva-norma-obliga-a-empresas-a-deshabilitar-telefonos-hurtados/>

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

- c) **Convenio de Budapest sobre Ciberdelincuencia.** Este tratado, ratificado por el Perú, obliga a los Estados a tipificar delitos informáticos y a establecer mecanismos de cooperación e investigación en el ciberespacio. Sus artículos 14 y 15 exigen que las medidas de investigación guarden respeto a los derechos humanos y a la proporcionalidad. La exposición de motivos del proyecto menciona que sus acciones deben alinearse con la implementación del Convenio de Budapest.

IV. ANALISIS DE LA PROPOSICIÓN LEGISLATIVA

4.1. Análisis técnico

El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) mantiene el Registro Nacional de Equipos Terminales Móviles para la Seguridad (Renteseq), donde se registran los reportes de equipos robados y bloqueados. De acuerdo con la información pública de OSIPTEL, los reportes de celulares robados han mostrado un pico en 2023 y una tendencia a la baja a partir de 2024:

Evolución de los robos de celulares reportados entre 2021 y 2025

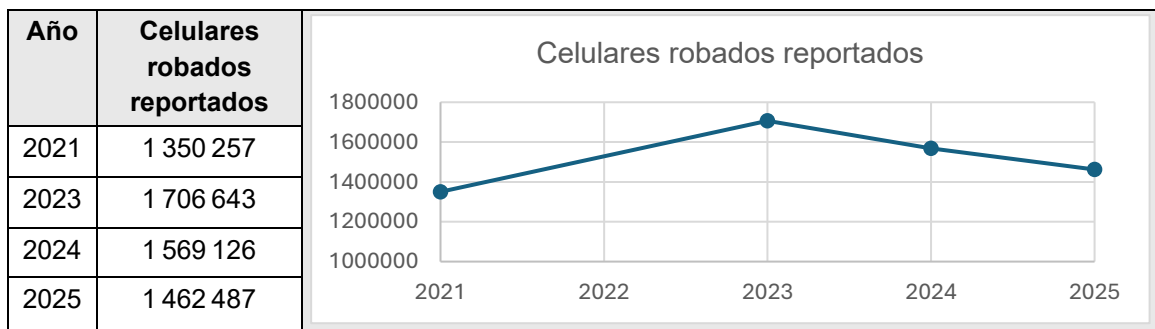


Figura 1. Tendencia de celulares robados reportados según OSIPTEL. El pico en 2023 corresponde a 1 706 643 reportes; en 2025, los reportes bajaron a 1 462 487.

Se observa un incremento entre 2021 y 2023, seguido de una disminución gradual. OSIPTEL señala que la reducción se debe a la aplicación más estricta de medidas de bloqueo de equipos y a la colaboración interinstitucional.

Los registros del Renteseq permiten identificar patrones diarios y semanales de robo. OSIPTEL destaca que la hora con mayor incidencia de robos en 2025 fue las 10:00 a.m., con un promedio de 287 celulares, seguida de las 11:00 a.m. (273) y las 7:00 p.m. (262). Estos picos coinciden con las horas de desplazamiento al trabajo y de retorno a casa.

La Figura 2 resume esta distribución horaria.

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

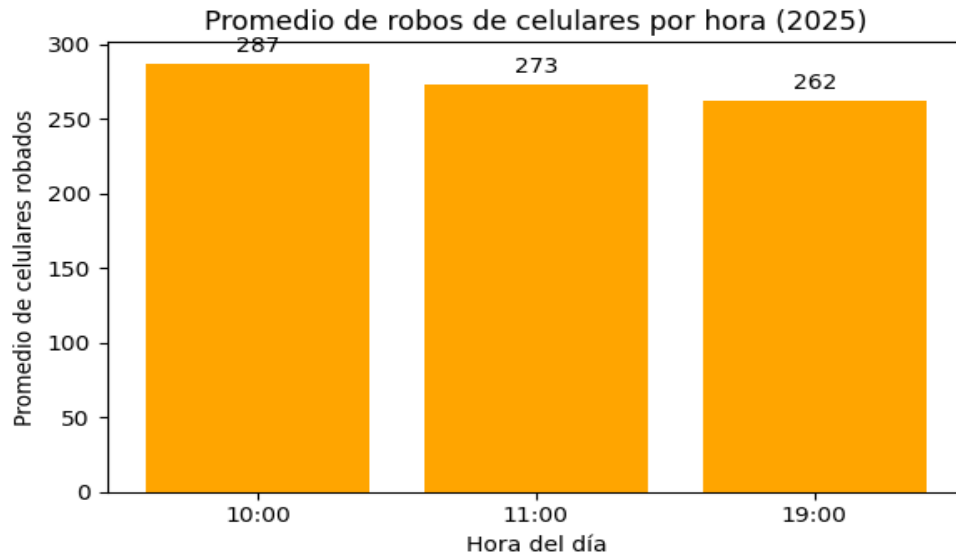


Figura 2. Promedio de celulares robados por hora, según datos de OSIPTEL para 2025. El pico de las 10 a.m. sugiere que los robos se concentran durante las horas de mayor movilidad de la población.

En cuanto a los días de la semana, OSIPTEL señala que los lunes concentran la mayor cantidad de reportes (4 846 celulares robados), seguidos por los sábados (4 194) y domingos (4 152).

La Figura 3 presenta esta distribución.

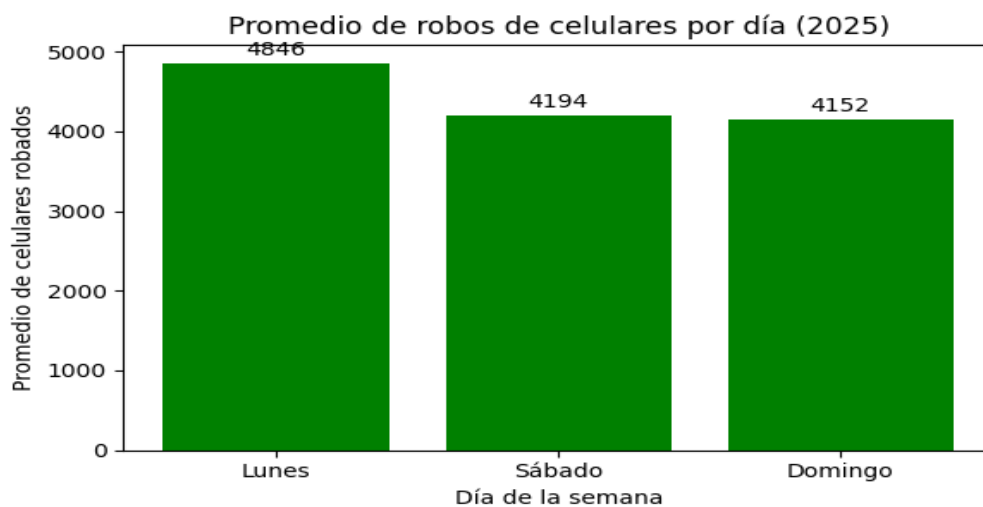


Figura 3. Promedio de celulares robados por día de la semana en 2025. La concentración en lunes indica que el inicio de la semana laboral es especialmente crítico.

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

La problemática del robo de celulares afecta a casi todo el país porque el uso de teléfonos móviles es generalizado. Según el Instituto Nacional de Estadística e Informática (INEI), en el primer trimestre de 2025 el 95,2 % de los hogares contaba con telefonía móvil y el 89,8 % de la población de 6 y más años utilizó un teléfono celular. La Encuesta Residencial de Servicios de Telecomunicaciones (Erestel) 2024 del OSIPTEL añade que el 94,8 % de los hogares peruanos dispone de un smartphone, superando incluso al televisor como el dispositivo más extendido.

El mismo estudio destaca que en 2024 el 99 % de los hogares de Lima Metropolitana tiene smartphone, mientras que en las zonas rurales la tenencia alcanzó el 84,8 %, lo que evidencia la rápida reducción de la brecha digital.

La Figura 4 resume estos resultados.

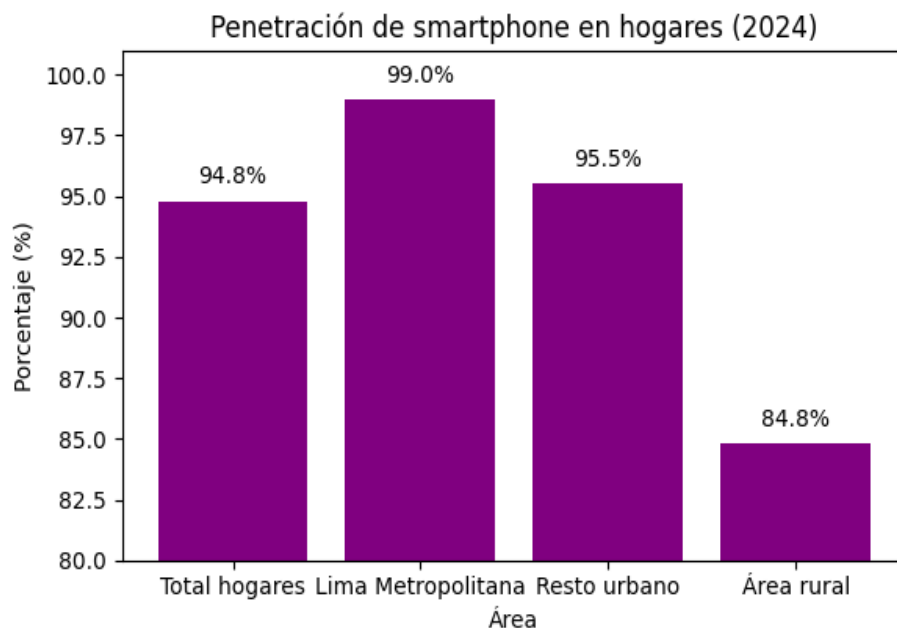


Figura 4. Porcentaje de hogares con smartphones según área geográfica (Erestel 2024). La tenencia casi universal de smartphones realza el impacto social del robo de celulares.

Un informe del Instituto Videnza y Lab-Co calculó que el costo anual del robo de celulares en el Perú alcanza S/ 2 171 millones, incluyendo el valor de los equipos, el tiempo perdido en trámites y los fraudes derivados de la suplantación de identidad⁶. El estudio identifica tres

⁶ Perú | Robo de celulares representa más de S/ 2,100 millones al año en costo de equipos para peruanos | INEI | Osipitel | ECONOMIA | GESTIÓN: <https://gestion.pe/economia/peru-robo-de-celulares-representa-mas-de-s-2100-millones-al-ano-en-costo-de-equipos-para-peruanos-inei-osipitel-noticia/>

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

motivaciones principales para este delito: reventa de equipos, comercialización de repuestos y uso de la información personal para cometer fraudes. La Figura 5 muestra una estimación de la proporción relativa de estas motivaciones.

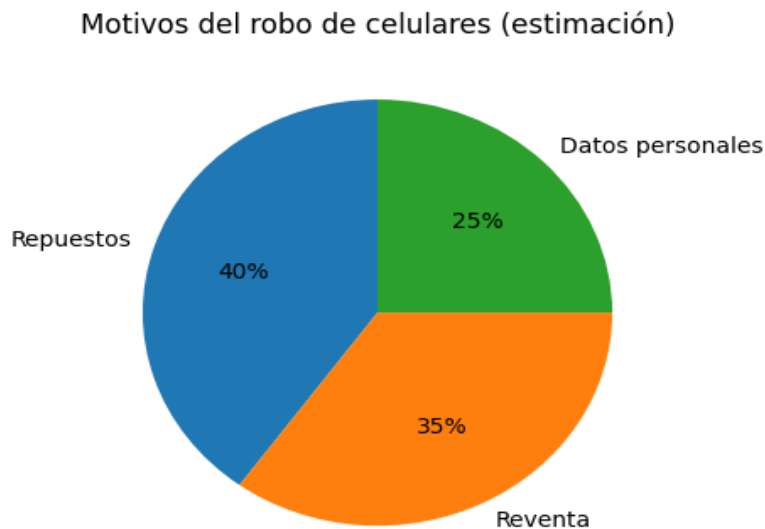


Figura 5. Principales motivaciones del robo de celulares. Aproximadamente 40 % de los robos busca repuestos, 35 % la reventa y 25 % la obtención de datos personales.

El robo de celulares no solo implica la pérdida del dispositivo sino también de información sensible almacenada en él: contraseñas, cuentas bancarias, registros de salud y documentos personales. La exposición de motivos del Proyecto de Ley 4247 advierte que con la información contenida en un celular robado se pueden cometer delitos como suplantación de identidad, transferencias bancarias no autorizadas y fraudes financieros. OSIPTEL añade que la cifra de líneas suspendidas por fraude (184 601 entre 2020 y 2023) demuestra la magnitud del problema.

Respecto del Proyecto de Ley 4247/2022-CR

El proyecto declara que su objeto es establecer medidas que garanticen la protección de la ciudadanía frente a los riesgos de seguridad digital derivados de la sustracción de equipos móviles y promover la confianza digital. Técnicamente, el objeto debe describir qué problema aborda y qué ámbito material cubre. La evidencia mostrada en la Sección 1 confirma que el robo de celulares es un problema significativo y que la confianza en la economía digital depende de la protección de datos de los usuarios.

Sin embargo, la redacción del objeto es imprecisa, utiliza el término "equipos móviles" en vez de "equipos terminales móviles" definido en el Decreto Legislativo 1338 y no delimita si las medidas se aplican sólo al robo o a cualquier delito informático. El MTC y la PCM señalan que es necesario ajustar el objeto para circunscribirlo al robo de celulares y evitar interpretaciones extensivas.

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

La finalidad de la ley consiste en disponer medidas sobre el uso de servicios, plataformas y tecnologías digitales para mitigar riesgos derivados de la sustracción de equipos móviles. Técnicamente, la finalidad debiera vincularse con el objeto y describir cómo las medidas contribuyen a la solución del problema. Aquí se hace referencia al uso de tecnologías digitales, pero no se especifica si las medidas son de prevención, de persecución o de remediación.

Con base en los datos de OSIPTEL y en las motivaciones del robo, la finalidad debería orientarse a disuadir el robo mediante bloqueo efectivo de equipos, prevenir el acceso a datos personales y facilitar la investigación de delitos de manera proporcional y respetuosa de la privacidad.

El artículo 3 permite que el Ministerio Público, el Poder Judicial y la Policía accedan a datos de identificación personal de bases de datos públicas y privadas "para permitir una respuesta oportuna" ante los delitos. Desde la perspectiva técnica, la norma presenta varios problemas:

- a) Falta de delimitación de las entidades y datos: la disposición autoriza el acceso a "datos de identificación personal" sin precisar qué datos (nombre, número de teléfono, historial de llamadas, geolocalización) ni qué entidades privadas (bancos, operadoras, tiendas) están obligadas a compartir información. La PCM advierte que la norma debe delimitar claramente el alcance para no vulnerar la Ley 29733.
- b) Ausencia de control judicial o consentimiento: la Constitución y la Ley de Protección de Datos exigen orden judicial o consentimiento expreso para acceder a datos personales. El MTC señala que la redacción actual permitiría que las entidades accedan a información sin autorización judicial, violando la privacidad y el secreto de comunicaciones.
- c) Desconocimiento de la plataforma PIDE: el Decreto Legislativo 1412 y el Decreto 1246 establecen que el intercambio de información entre entidades públicas se realiza mediante la Plataforma de Interoperabilidad del Estado Peruano (PIDE), con garantías de seguridad y trazabilidad. El proyecto no menciona la PIDE ni la Autoridad Nacional de Protección de Datos (ANPD). Implementar un nuevo sistema de intercambio duplicaría funciones y aumentaría costos sin aportar valor.
- d) Riesgos de ciberseguridad: centralizar la información de bases de datos públicas y privadas podría generar un objetivo atractivo para ciberdelincuentes. La experiencia muestra que los datos robados pueden ser utilizados para fraudes y suplantación de identidad. Cualquier sistema de intercambio debe incluir estándares de seguridad equivalentes a los recomendados por la Ley de Gobierno Digital y normas ISO 27001.

Dada la alta penetración de smartphones en la población, la posibilidad de que millones de datos personales se compartan sin control judicial representa un riesgo elevado. Se recomienda restringir la interoperabilidad al PIDE, establecer que sólo se acceda a datos

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

mediante orden judicial y garantizar la trazabilidad del acceso, manteniendo registros auditables de quién consulta la información y para qué finalidad.

El artículo 4 propone que entidades públicas y privadas promuevan tecnologías que permitan bloquear de manera remota equipos terminales robados. El objetivo parece alinearse con las tendencias internacionales de kill switch.

El proyecto dispone que la implementación se financia con el presupuesto institucional de las entidades públicas. Dado que la propuesta plantea crear plataformas adicionales y ampliar el alcance de la interoperabilidad, resulta imprescindible un análisis de impacto presupuestal. Las experiencias comparadas indican que el desarrollo de plataformas de seguridad digital requiere inversión en infraestructura tecnológica, ciberseguridad y capacitación; sin un financiamiento específico, las entidades podrían desatender otras prioridades.

El reglamento debe elaborarse con participación de la PCM, el MTC, OSIPTEL y la ANPD para garantizar coherencia con las normas existentes. Además, la norma debe incluir un periodo de implementación gradual para ajustar procesos y sistemas.

El proyecto modifica los artículos 6 y 8 del Decreto Legislativo 1338 y deroga su artículo 5. Técnicamente, estas modificaciones generan las siguientes implicancias:

- e) Artículo 6. Permitir que el Ministerio Público, la Policía y el Poder Judicial accedan a la información del RENTASEG mediante interoperabilidad facilitaría la investigación de delitos. Sin embargo, como se analizó en el artículo 3, el acceso debe pasar por la PIDE y requerir orden judicial.
- f) Artículo 8. La obligación de las operadoras de verificar la identidad del usuario mediante biometría u otras tecnologías ya existe en el Decreto 1338. El proyecto sugiere reforzarla, pero no incluye a OSIPTEL como autoridad de supervisión. Técnicamente, se recomienda que OSIPTEL valide las tecnologías de verificación y que las actualice periódicamente para prevenir suplantaciones.
- g) Derogación del artículo 5. Este artículo obliga a los operadores a bloquear los equipos reportados como robados. Derogarlo sin reemplazarlo adecuadamente debilitaría el RENTASEG y dejaría desprotegidos a los usuarios. Tanto la PCM como el MTC rechazan la derogación.

El proyecto debe armonizar con la Constitución y Ley de Protección de Datos Personales: cualquier acceso a datos personales debe ser legal, necesario y proporcional. Ley de Gobierno Digital (D.L. 1412), establece que la interoperabilidad se realiza mediante la PIDE y que la PCM es responsable de la gobernanza digital. El proyecto no menciona esta plataforma ni su coordinación con la ANPD.

Asimismo, otro aspecto importante son las leyes de kill switch en Minnesota y California obligan a fabricantes a incluir la función, mientras que la ley chilena exige a las operadoras bloquear equipos robados en 24 horas. El proyecto podría inspirarse en estos precedentes para reforzar la obligación de bloqueo sin duplicar estructuras. Decisión 786 de la Comunidad

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

Andina: impone el intercambio de información sobre equipos robados entre países miembros. La propuesta debe articularse con esta decisión y con las obligaciones del RENTESEG.

4.2. Análisis sobre la necesidad, viabilidad y oportunidad de la propuesta legislativa

a) Sobre la necesidad:

La iniciativa legislativa, aborda un problema público evidente que viene incrementando en los últimos años en el Perú. El robo de celulares constituye un fenómeno generalizado. La exposición de motivos menciona que en el 2021 se registraron más de 1,35 millones de celulares robados y que el 82 % de los delitos patrimoniales se relacionan con la sustracción de celulares.

OSIPTEL reportó que en el 2023 se robaron 1 706 643 celulares (4 676 al día) y que desde 2018 se han realizado 14,5 millones de bloqueos de equipos con IMEI inválido⁷. Un estudio del Instituto Videnza y LAB-CO cifró el costo anual del robo de celulares en aproximadamente S/ 2 171 millones y señaló que 15 de cada 100 peruanos han sido víctimas de este delito. Estos datos evidencian la necesidad de fortalecer la respuesta estatal frente al robo de equipos y el uso indebido de datos personales.

La Encuesta Residencial de Servicios de Telecomunicaciones (Erestel) 2024, señala que el 94,8 % de los hogares peruanos dispone de un smartphone y que en Lima Metropolitana la tenencia llega al 99 %, mientras que en zonas rurales alcanza el 84,8 %. La casi universalidad de estos dispositivos evidencia que el robo de celulares afecta de manera transversal a la sociedad. Adicionalmente, el Instituto Nacional de Estadística e Informática (INEI) estima que el 95,2 % de los hogares cuenta con telefonía móvil y que el 89,8 % de la población mayor de seis años utiliza un teléfono celular. La combinación de una alta penetración de smartphones y un elevado número de robos convierte este delito en un problema de seguridad ciudadana y ciberseguridad.

Actualmente, el Decreto Legislativo 1338 creó el Registro Nacional de Equipos Terminales Móviles (Renteseq) y obliga a las empresas operadoras a verificar la identidad del usuario mediante verificación biométrica (huella dactilar) y a bloquear los equipos reportados como robados. El Decreto Supremo N° 007-2019-IN reglamentó estas obligaciones. Además, la Plataforma de Interoperabilidad del Estado (PIDE), administrada por la Secretaría de Gobierno y Transformación Digital de la PCM, permite que las entidades públicas intercambien información de manera segura.

Sin embargo, es importante reconocer que las medidas existentes han sido insuficientes. Aunque el Renteseq registra y bloquea equipos, el alto número de robos

⁷ OSIPTEL: ¿qué días se reportaron más robos de celulares durante 2023?
<https://www.osiptel.gob.pe/portal-del-usuario/noticias/osiptel-qu%C3%A9-d%C3%ADas-se-reportaron-m%C3%A1s-robos-de-celulares-durante-2023/>

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

revela que los delincuentes desactivan o alteran el IMEI, venden el dispositivo en mercados informales o utilizan los repuestos. La verificación biométrica no ha evitado el robo, y la información personal de las víctimas sigue expuesta. Asimismo, los organismos encargados de investigar (Ministerio Público y Policía) enfrentan barreras para acceder rápidamente a datos personales que permitan identificar a los responsables. Las disposiciones del D.L. 1338 se orientan a la desactivación de equipos, pero no abordan la necesidad de coordinar la persecución penal ni la protección de datos.

Ante este panorama, la iniciativa legislativa propone reforzar el control y la cooperación interinstitucional. El problema no es solo técnico (bloqueo de IMEI) sino legal y organizativo. Se requiere un marco que obligue a los operadores, proveedores de servicios y organismos públicos a compartir información de manera oportuna y a incorporar mecanismos de "kill switch" (bloqueo remoto) en los dispositivos. Además, es fundamental incorporar salvaguardas que protejan la privacidad de los ciudadanos. La combinación de estos elementos (bloqueo, cooperación e investigación) justifica la necesidad de una ley que actualice el régimen de seguridad digital.

b) Sobre la viabilidad:

El proyecto autoriza al Ministerio Público, la Policía y el Poder Judicial a acceder a datos de identificación personal almacenados en bases de entidades públicas y privadas. Para que esta disposición sea viable, debe cumplir con el principio de proporcionalidad: el acceso a la información debe ser necesario para la investigación, adecuado para el fin perseguido y proporcional (no debe exceder lo estrictamente necesario).

Es importante, exigir una orden judicial para acceder a datos personales, se debe establecer que el Ministerio Público, la Policía y el Poder Judicial podrán acceder al Renteseg y a otras bases "exclusivamente a través de la PIDE y previa autorización judicial". Además, hay que señalar que cualquier intercambio con organizaciones privadas requerirá el consentimiento expreso del titular de los datos o mandato judicial y que se sujetará a la Ley 29733 (Ley de Protección de Datos Personales). Estas modificaciones responden a las observaciones de la PCM y el MTC sobre la vulneración del derecho a la intimidad.

El Decreto Legislativo 1338 y su reglamento ya obligan a las operadoras a bloquear el IMEI de equipos robados y a suspender la línea telefónica. Asimismo, en mercados como Estados Unidos (Minnesota y California) la legislación exige a los fabricantes incorporar un "kill switch" que permita al usuario desactivar el dispositivo de manera irreversible. La evidencia comparada muestra que en ciudades como San Francisco los robos de smartphones se redujeron 50 % entre 2013 y 2017 tras la implementación de esta medida.

La iniciativa legislativa incorpora esta experiencia al exigir que los fabricantes de dispositivos que comercialicen equipos en el país incluyan mecanismos de bloqueo

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

remoto y borrado seguro, lo cual no estaba contemplado en el D.L. 1338. Además, el texto sustitutorio precisa que el MTC y OSIPTEL establecerán los requisitos técnicos mínimos de estas funciones. En ese sentido, la medida es técnicamente viable y no generaría costos excesivos; simplemente obligará a los proveedores a habilitar la función y a informar al usuario.

La propuesta mantiene y refuerza el Renteseq al permitir que el Ministerio Público y el Poder Judicial accedan a la base de datos mediante la PIDE, previa orden judicial. Asimismo, la modificación del artículo 8 del D.L. 1338 plantea que la verificación biométrica del usuario sea obligatoria y que cualquier tecnología alternativa de autenticación ofrezca niveles de seguridad equivalentes y cuente con la evaluación técnica y autorización del MTC y OSIPTEL. Esta precisión responde a la preocupación de la PCM y el MTC de que la ley permitiera verificación "de similar seguridad" sin control. El asegurar que OSIPTEL supervise las tecnologías reduce el riesgo de suplantación.

c) Sobre la oportunidad:

La percepción de inseguridad en el Perú se ha agravado debido al aumento de delitos como el robo de celulares, la extorsión y la ciberdelincuencia. La Fiscalía de la Nación ha destacado que la sustracción de equipos móviles no sólo genera pérdidas económicas, sino que sirve de base para otros delitos (robo de identidad, extorsión, fraude). La ciudadanía exige medidas inmediatas que no sólo bloqueen los equipos, sino que identifiquen y sancionen a los responsables. En este contexto, una ley que fortalezca la confianza digital y coordine la actuación de las entidades públicas es sumamente pertinente.

El Perú se encuentra inmerso en un proceso de transformación digital que exige interoperabilidad, identidad digital segura y protección de datos personales. El Decreto Legislativo 1412 (Ley de Gobierno Digital) establece la PIDE como la herramienta principal para el intercambio de información entre entidades públicas y la digitalización de servicios. La agenda legislativa 2024-2025 incorpora como política de Estado la "sociedad de la información y del conocimiento". La aprobación de una ley que refuerce la seguridad digital y el bloqueo de equipos robados se alinea con esta agenda y demuestra que la digitalización debe ir acompañada de medidas de seguridad.

El Perú es parte de la Decisión 786 de la Comunidad Andina, que obliga al intercambio de información sobre equipos móviles robados entre los países miembros, y del Convenio de Budapest sobre Ciberdelincuencia, que exige tipificar delitos informáticos y garantizar que las medidas de investigación respeten los derechos humanos. La iniciativa legislativa complementa estos compromisos al reforzar el intercambio de datos (con autorización judicial) y al exigir que los fabricantes incorporen herramientas de bloqueo. Dado que el crimen organizado que roba celulares opera a nivel regional, la

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

articulación con normas andinas y acuerdos internacionales es un argumento a favor de la oportunidad de la ley.

4.3. Análisis del marco normativo y efecto de la vigencia de la norma

La Constitución Política del Perú reconoce el derecho a la intimidad, a la protección de los datos personales y el secreto de las comunicaciones (art. 2, incisos 6 y 10). Estas garantías solo pueden limitarse mediante ley y con respeto a los principios de legalidad, necesidad y proporcionalidad. El Ministerio Público y la Policía Nacional del Perú, por su rol en la persecución penal, pueden acceder a información personal solo con autorización judicial, salvo excepciones expresas señaladas en la Constitución.

De igual manera, la Ley 29733, Ley de Protección de Datos Personales, establece que el tratamiento de datos requiere consentimiento o mandato legal, y obliga a las entidades a adoptar medidas de seguridad. Cualquier norma que habilite el acceso a datos debe prever salvaguardas para evitar vulneraciones.

El Decreto Legislativo 1412, Ley de Gobierno Digital, crea la Plataforma de Interoperabilidad del Estado (PIDE) y dispone que el intercambio de información entre entidades públicas se realice a través de ella bajo estándares de seguridad. La autoridad de gobernanza digital es la Secretaría de Gobierno y Transformación Digital de la PCM.

Mientras que el Decreto Legislativo 1338 y su Reglamento (D.S. 007-2019-IN); establece el Registro Nacional de Equipos Terminales Móviles (RENTESEG), regula la verificación biométrica de usuarios y obliga a las operadoras a bloquear los equipos robados y suspender las líneas asociadas. La norma incorpora la Decisión 786 de la Comunidad Andina, que obliga a intercambiar información sobre IMEI entre países miembros.

Asimismo, la normativa internacional, respecto a leyes de "kill switch" en Minnesota y California (Estados Unidos) y la ley chilena de bloqueo de equipos en 24 horas inspiran medidas técnicas de bloqueo y borrado remoto. Del mismo modo, el Convenio de Budapest sobre Ciberdelincuencia y la Convención Americana sobre Derechos Humanos exigen que las medidas de investigación respeten la privacidad y sean proporcionadas.

El impacto de la propuesta normativa será positivo y permitirá brindar seguridad ciudadana y reducción del delito, toda vez que logrará reforzar el bloqueo de equipos, habilitar el "kill switch" y facilitar la coordinación entre autoridades, se espera que el robo de celulares disminuya significativamente, como ocurrió en Estados Unidos y Chile. La reducción de la demanda de equipos robados y la trazabilidad de los datos generarán un efecto disuasivo.

Se garantiza el fortalecimiento de la investigación penal, con acceso controlado a la base RENTESEG mediante la PIDE, el Ministerio Público y la Policía podrán identificar

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

rápidamente los movimientos de los equipos robados y la identidad de los usuarios, reduciendo los plazos de investigación y aumentando la probabilidad de sancionar a las bandas delictivas.

La exigencia de orden judicial y el uso de la PIDE aseguran que la norma sea compatible con la Constitución y la Ley de Protección de Datos. Las intervenciones en datos personales se justifican por la finalidad legítima de perseguir delitos y se realizan bajo control judicial, cumpliendo el principio de proporcionalidad.

La vigencia de la norma demandará inversiones tecnológicas y capacitación en las entidades públicas y operadoras. Será necesario fortalecer la ciberseguridad de la PIDE para evitar ataques que puedan vulnerar las bases de datos. Además, el Ministerio Público deberá ajustar sus procedimientos para solicitar órdenes judiciales y garantizar la debida diligencia.

4.4. Análisis de las opiniones e información solicitadas

Opiniones solicitadas:

Fecha de envío	Institución	Documento
17/05/2024	Ministerio de Transportes y Comunicaciones	Oficio N° 1569-2023-2024-CTC-CR.
17/05/2024	Fiscalía de la Nación	Oficio N° 1570-2023-2024-CTC-CR.
17/05/2024	Poder Judicial	Oficio N° 1571-2023-2024-CTC-CR.
17/05/2024	Ministerio del Interior	Oficio N° 1572-2023-2024-CTC-CR.
17/05/2024	Presidencia del Consejo de Ministros	Oficio N° 1573-2023-2024-CTC-CR.
17/05/2024	Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL.	Oficio N° 1574-2023-2024-CTC-CR.

Elaboración: Comisión de Transportes y Comunicaciones

Opiniones recibidas:

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

Fecha de envío	Institución	Documento
24/10/2023	Presidencia del Consejo de Ministros	Oficio N° D002926-2023-PCM-SG
27/09/2024	Poder Judicial	Oficio N° 004263-2024-SG-CS-PJ
08/04/2025	Ministerio de Transportes y Comunicaciones	Oficio N° 057-2025-MTC/01
09/08/2024	Ministerio Público	Oficio N° 003721-2024-MP-FN-SEGFN

Elaboración: Comisión de Transportes y Comunicaciones

Análisis de las opiniones recibidas del Proyecto de Ley 4247/2022-CR

- **Presidencia del Consejo de Ministros:** El informe de la PCM señala que, aunque la iniciativa busca aumentar la confianza digital, no justifica adecuadamente la necesidad ni la viabilidad de las medidas propuestas. La exposición de motivos debería describir el problema, analizar la situación jurídica actual, evaluar el costo-beneficio y fundamentar con datos por qué se requiere una ley.

La PCM concluye que el proyecto no es viable, por falta de justificación y porque invade competencias de los ministerios de Transportes y Comunicaciones, Interior y Justicia. Entre sus comentarios y observaciones destacan:

- Ámbito y redacción de los artículos 1 y 2. Sugiere acotar el objeto y finalidad de la ley conforme al Manual de Técnica Legislativa, pues el artículo 1 resume un objetivo general y el artículo 2 contiene elementos del objeto y de la finalidad; ambos deben diferenciarse claramente.
- Artículo 3. Indica que el alcance es demasiado amplio al referirse a "entidades privadas" sin delimitar qué tipos de entidades deben cumplir con las obligaciones de interoperabilidad; recomienda precisar qué entidades estarían obligadas y en qué supuestos. También propone aclarar a qué se refiere "equipos móviles o similares" y la naturaleza de los datos a intercambiar. Señala que la plataforma PIDE ya permite la interoperabilidad entre entidades públicas y que podría aprovecharse en lugar de crear una nueva disposición.
- Artículo 4. La PCM observa que el Reglamento del Decreto

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

Legislativo 1338 ya obliga a las empresas operadoras a bloquear y suspender servicios de telefonía móvil de manera inmediata cuando se reporta un equipo robado. Por ello, considera innecesario establecer en la ley medidas técnicas de seguridad que ya forman parte de la normativa vigente.

- d) Modificación del artículo 5 del Decreto Legislativo 1338. La PCM no formula observaciones, ya que la derogación del artículo 5 coincide con su postura.
 - e) Modificación del artículo 6. Señala que es redundante impulsar un nuevo acceso digital al RENTASEG porque el Ministerio Público y el Poder Judicial ya pueden consultar dicha base a través de la plataforma PIDE.
 - f) Modificación del artículo 8. Le preocupa que la propuesta permita que la verificación de la identidad del usuario sea mediante tecnologías de "similar seguridad" sin un control externo. Recomienda ajustar la redacción para que cualquier tecnología alternativa sea evaluada y aprobada por una entidad técnica y el OSIPTEL.
- **Ministerio de Transportes y Comunicaciones:** El informe N° 0156-2024-MTC/26 analiza cada artículo del proyecto y advierte que varias disposiciones ya se encuentran reguladas en la normativa de telecomunicaciones. Sus principales observaciones son:
 - a) Artículos 1 y 2: objeto y finalidad. El MTC señala que el proyecto utiliza el término "equipos móviles" de manera imprecisa. Recuerda que la normativa sectorial define "equipo terminal móvil" y "teléfono celular" como dispositivos que poseen IMEI y permiten acceder a servicios públicos de telecomunicaciones. Sugiere que la ley utilice las definiciones vigentes para delimitar el ámbito de aplicación. Además, observa que los artículos 1 y 2 son meramente enunciativos y no agregan contenido normativo sustantivo, por lo que su redacción podría ajustarse o integrarse.
 - b) Artículo 3 – Intercambio de información. El informe advierte que el numeral 3.1 autoriza el acceso a bases de datos públicas y privadas sin especificar qué entidades deben proporcionar información ni qué datos pueden entregarse. Esto podría obligar a cualquier entidad pública o privada a entregar datos que no guardan relación con el objeto de la ley. El MTC destaca que tal obligación podría vulnerar derechos fundamentales, como la autodeterminación informativa, la intimidad y la inviolabilidad de las comunicaciones. Recomienda delimitar el alcance del artículo, establecer criterios claros para la información que se requiere y condicionar el acceso

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

a supuestos legales específicos, como una orden judicial. También señala que la plataforma PIDE ya permite el intercambio de información entre entidades públicas, por lo que sería redundante establecer un nuevo mecanismo.

- c) Artículo 4. Medidas técnicas de seguridad digital. El MTC recuerda que el Decreto Supremo N.º 007-2019-IN (Reglamento del D.L. 1338) obliga a las empresas operadoras a bloquear la línea y el IMEI inmediatamente luego de que el usuario reporte el hurto de un equipo. Además, resalta que los fabricantes ya incorporan mecanismos como el "kill switch" que permiten al usuario bloquear o borrar información del terminal de manera remota y que existen aplicaciones disponibles para localizar y desactivar dispositivos robados. Por ello, considera que el artículo 4 es innecesario y duplica obligaciones vigentes.
- d) Modificación de los artículos 5, 6 y 8 del D.L. 1338. El MTC no observa la derogación del artículo 5. Respecto al artículo 6, coincide con la PCM en que el Ministerio Público y el Poder Judicial ya tienen acceso al RENTASEG a través de la plataforma PIDE, por lo que no es necesario crear un nuevo mecanismo. Para la modificación del artículo 8, señala que la verificación biométrica de la identidad de los usuarios ya es obligatoria y que cualquier tecnología alternativa debe garantizar niveles de seguridad equivalentes y ser aprobada por la autoridad competente (OSIPTel y MTC).
- **Poder Judicial:** señala que, resulta evidente que el Poder Judicial, no tiene competencia ni atribuciones sobre la citada Ley, en tanto que esta depende para su ejecución y/o implementación de la Presidencia del Consejo de Ministros, OSIPTel, Ministerio del Interior y la Policía Nacional del Perú, siendo estos órganos a los que se deberán requerir la opinión respectiva de considerarlo pertinente.

En tal sentido, resulta claro que el proyecto de Ley no afecta en sí mismo a los procesos penales o a la actividad jurisdiccional que efectúa este Poder Judicial, por lo cual no resulta de competencia de este Poder del Estado sino y, como ya se señaló previamente, corresponde a las instituciones del Poder Ejecutivo.

- **Ministerio Público:** La Fiscalía avala técnica y jurídicamente el proyecto de ley en casi todos sus extremos, reconociendo su contribución a la seguridad ciudadana, la protección de datos personales y la investigación penal.

El informe reafirma el rol constitucional del Ministerio Público en: (i) Conducción de la investigación del delito, (ii) Prevención del delito y el (iii) Acceso razonable a

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

información para fines penales. No se advierte vulneración de derechos fundamentales cuando el acceso a datos se realiza bajo principios de legalidad y proporcionalidad.

Se considera estratégico ampliar el acceso al RENTASEG al Ministerio Público y al Poder Judicial, lo que reduce tiempos de investigación, mejora la trazabilidad de equipos robados y fortalece la persecución penal.

La Fiscalía rechaza expresamente la derogación del artículo 5 del Decreto Legislativo 1338, señalando que; es una medida de seguridad, no una restricción ilegítima a la propiedad. Su eliminación debilitaría el control estatal e incrementaría la criminalidad asociada a celulares. En ese sentido, respalda técnicamente la competencia de la Comisión. Justifica el fortalecimiento normativo del sistema de control de equipos móviles.

La siguiente tabla resume los principales puntos de coincidencia y divergencia entre la Fiscalía, la PCM y el MTC:

Aspecto	Fiscalía	PCM	MTC
Necesidad de la ley	Avala la ley; considera que fortalece la investigación penal y protege datos.	Considera que la necesidad no está adecuadamente justificada; falta análisis costo-beneficio y definición clara del problema.	Cuestiona la necesidad de duplicar disposiciones existentes; propone precisar definiciones.
Acceso a datos personales	Apoya ampliar el acceso a Renteseg para el Ministerio Público y el Poder Judicial, con principios de legalidad y proporcionalidad.	Critica la amplitud del artículo 3; demanda delimitar entidades y datos, y utilizar la PIDE con orden judicial.	Observa que el acceso a bases debe ser limitado, con orden judicial y uso de PIDE.
Bloqueo y kill switch	Considera que el bloqueo de equipos es una medida de seguridad indispensable y rechaza la derogación del art. 5 del D.L. 1338.	Señala que las medidas de bloqueo ya están en la normativa; ve redundancia.	Coincide con la PCM; sostiene que el reglamento ya obliga al bloqueo y que los fabricantes incorporan kill switch.
Verificación biométrica	Apoya reforzar la verificación e incluir tecnologías alternativas	Sugiere que el proyecto no permita tecnologías sin control;	Coincide en exigir aprobación técnica y

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

Aspecto	Fiscalía	PCM	MTC
	aprobadas técnicamente.	requiere supervisión de OSIPTEL/MTC.	supervisión por OSIPTEL/MTC.

La divergencia fundamental reside en la validez y alcance de la propuesta. Mientras la Fiscalía ve la ley como una herramienta necesaria para la persecución penal, la PCM y el MTC la consideran innecesaria o redundante en algunos aspectos. No obstante, ambos órganos coinciden en que la normativa debe garantizar la privacidad, delimitar claramente sus alcances y aprovechar las plataformas existentes

4.5. Análisis costo beneficio

El robo de celulares genera pérdidas económicas para los ciudadanos y el Estado. La OSIPTEL reportó que en 2023 se robaron 1 706 643 celulares en el Perú (4 676 al día). Un estudio del Instituto Videnza estima que el costo anual de este delito asciende a S/ 2 171 millones, considerando el valor de los dispositivos y los perjuicios derivados de la suplantación de identidad y la pérdida de información. El estudio identifica tres motivaciones para el robo; reutilizar los aparatos como repuestos, revenderlos ilegalmente y utilizar la información para cometer fraudes electrónicos.

Las leyes de kill switch en Estados Unidos demostraron una reducción significativa del robo de smartphones; en San Francisco, la tasa de robos disminuyó 50 % tras la entrada en vigor de la legislación. Si se implementan correctamente mecanismos de bloqueo y un registro centralizado, se podría reducir la demanda de dispositivos robados y los costos sociales asociados. La mejora de la confianza digital también podría incentivar la economía digital y reducir el costo de la ciberdelincuencia.

Para alcanzar un equilibrio entre costos y beneficios, la propuesta legislativa debería:

- Fortalecer el RENTEG y la obligación de los operadores de bloquear equipos reportados sin derogar las disposiciones vigentes.
- Limitar el intercambio de información a lo estrictamente necesario, utilizando la PIDE como plataforma y exigiendo orden judicial para acceder a datos sensibles, a fin de cumplir con la Ley 29733 y los tratados internacionales.
- Promover la adopción de kill switch mediante acuerdos con fabricantes y campañas de sensibilización, sin imponer obligaciones difíciles de supervisar a operadores o usuarios. La experiencia de California y Minnesota puede servir como referencia.

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

Es importante señalar que, tanto la PCM como el MTC destacan que varias de las medidas propuestas ya están reguladas. Las normas sobre bloqueo de equipos robados (IMSI/IMEI), suspensión de líneas y sistemas de bloqueo por software (kill switch) son obligaciones vigentes para los operadores. Crear otra disposición legal que ordene lo mismo generaría duplicidad y podría generar confusión en su aplicación.

El artículo 3 del proyecto permite a los órganos de persecución penal acceder a bases de datos públicas y privadas mediante interoperabilidad. Sin embargo, no delimita qué entidades deben proporcionar información ni qué datos pueden ser intercambiados, lo que podría afectar derechos como la autodeterminación informativa, la intimidad y la inviolabilidad de las comunicaciones.

Cualquier regulación que habilite el acceso a datos personales debe contar con un fundamento legal preciso y cumplir con el test de proporcionalidad: la medida debe ser necesaria, idónea y proporcional al fin perseguido. Además, la Ley de Protección de Datos Personales establece que solo puede levantarse la confidencialidad de datos con consentimiento del titular, orden judicial o razones de defensa nacional o seguridad pública. Las medidas propuestas involucran competencias del MTC (infraestructura y servicios de telecomunicaciones), del Ministerio del Interior (orden interno y seguridad ciudadana) y del Ministerio de Justicia y Derechos Humanos (protección de datos personales). Cualquier regulación sobre interoperabilidad de bases de datos y bloqueo de equipos requiere la participación de estas entidades y de OSIPTEL.

Entre los principales beneficios de la presente propuesta normativa tenemos:

- Reducción del robo de celulares: Las leyes de "kill switch" implementadas en países como Estados Unidos demostraron que el robo de smartphones disminuyó hasta un 50 % tras la entrada en vigor de la obligación de bloqueo remoto. Si en Perú se refuerzan el Renteseq y el bloqueo de IMEI, y se obliga a los fabricantes a incorporar un "kill switch" de fábrica, se espera que la demanda de dispositivos robados disminuya y, con ella, el incentivo para robar celulares.
- Protección de datos personales: El acceso a datos mediante la PIDE, previa orden judicial, permitirá al Ministerio Público y a la Policía identificar a los delincuentes sin vulnerar la privacidad de los ciudadanos. La obligación de usar tecnologías de autenticación biométrica controladas por OSIPTEL evitará la activación de líneas con identidades falsas. Además, los mecanismos de borrado remoto reducirán el valor de la información robada.
- Mejora de la confianza digital y del comercio electrónico: Si los ciudadanos perciben que sus datos están protegidos y que las autoridades pueden rastrear

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

y sancionar a los responsables, estarán más dispuestos a realizar transacciones digitales. Esto beneficia no solo a los usuarios sino también al ecosistema de negocios electrónicos.

- Mejor cooperación interinstitucional: Al centralizar el intercambio de información en la PIDE, se facilita la coordinación entre el Ministerio Público, el Poder Judicial, el MTC, el OSIPTEL y las empresas operadoras. La disposición que obliga a elaborar lineamientos técnicos de interoperabilidad en 90 días fomentará la claridad y la transparencia.

La Fiscalía de la Nación emitió un pronunciamiento favorable al proyecto de ley. En su informe señala que el proyecto contribuye a la seguridad ciudadana y a la protección de datos personales y afirma que el acceso a la información por parte del Ministerio Público no vulnera derechos fundamentales cuando se realiza bajo los principios de legalidad y proporcionalidad. Además, considera estratégico que el Ministerio Público y el Poder Judicial tengan acceso al Renteseq para reducir los tiempos de investigación y fortalecer la persecución penal. La Fiscalía rechaza, sin embargo, la derogación del artículo 5 del Decreto Legislativo 1338, pues lo considera una medida de seguridad indispensable para evitar la reactivación de equipos robados.

V. CONCLUSION

Por lo expuesto, la Comisión de Transportes y Comunicaciones, de conformidad con el literal b) del artículo 70 del Reglamento del Congreso de la República, recomienda la **APROBACIÓN** del Proyecto de Ley 4247/2022-CR con el siguiente **TEXTO SUSTITUTORIO**:

LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA FRENTE A LA SUSTRACCIÓN DE EQUIPOS TERMINALES MÓVILES Y FORTALECER LA CONFIANZA DIGITAL

Artículo 1. Objeto de la Ley

La presente ley tiene por objeto establecer medidas destinadas a prevenir y mitigar los riesgos de seguridad digital derivados de la retención ilegal de equipos terminales móviles, comprendiendo dentro de dicho concepto el hurto, robo, apropiación ilícita u otras modalidades de obtención indebida.

Artículo 2. Finalidad de la Ley

La presente ley tiene por finalidad fortalecer la seguridad ciudadana y la confianza digital mediante mecanismos de coordinación interinstitucional entre la Policía Nacional del Perú, el Ministerio del Interior, el Ministerio de Transportes y Comunicaciones, el Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL, las empresas operadoras de servicios públicos de telecomunicaciones y los fabricantes de equipos terminales móviles,

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

con el objeto de garantizar el bloqueo, localización y recuperación oportuna de equipos terminales móviles sustraídos de manera ilegal, y prevenir y sancionar su comercialización ilegal asegurando el respeto del derecho a la privacidad y a la protección de datos personales.

Artículo 3. Acceso a información para la investigación de delitos

- 3.1. El Ministerio Público, la Policía Nacional del Perú y el Poder Judicial, en el marco de investigaciones por delitos relacionados con la sustracción de equipos terminales móviles, pueden acceder a la información contenida en el Registro Nacional de Equipos Terminales Móviles para la Seguridad (RENTESEG), y en otras bases de datos estatales relacionadas, exclusivamente a través de la Plataforma de Interoperabilidad del Estado (PIDE) y previa autorización judicial, conforme a la normativa sobre protección de datos personales y secreto de las comunicaciones.
- 3.2. Las entidades públicas y las empresas operadoras de servicios públicos móviles deben facilitar la interoperabilidad de sus sistemas con la PIDE para proporcionar la información estrictamente necesaria indicada en el requerimiento judicial, garantizando la trazabilidad de los accesos y el respeto de la confidencialidad de los datos.
- 3.3. Cualquier intercambio de información con las empresas operadoras de servicios públicos móviles no comprendidas en el párrafo 3.2 requiere el consentimiento expreso del titular de los datos o mandato judicial, y se sujeta a las disposiciones de la Ley 29733, Ley de Protección de Datos Personales.
- 3.4. El Ministerio de Transportes y Comunicaciones (MTC), el Ministerio del Interior y el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) elaboran, en un plazo de noventa días hábiles contados desde la entrada en vigor de la ley, los lineamientos técnicos para el intercambio de información previsto en este artículo.

Artículo 4. Medidas de bloqueo y rastreo de equipos terminales móviles

- 4.1. Las empresas operadoras de servicios públicos móviles están obligadas a bloquear de manera inmediata el código IMEI y la línea asociada de los equipos terminales móviles que sean reportados como robados o perdidos por el abonado, su representante o el usuario, conforme al Reglamento del Decreto Legislativo 1338. El bloqueo impedirá el uso del equipo en cualquier red nacional e internacional.
- 4.2. Los fabricantes de equipos terminales móviles que comercialicen dispositivos en el país deben incorporar funciones nativas de bloqueo remoto y borrado seguro ("kill switch") que permitan al usuario desactivar el equipo en caso de robo o pérdida. El MTC y el OSIPTEL establecen los requisitos técnicos mínimos y la forma de activación de estas funciones.

Artículo 4. Medidas de bloqueo y rastreo de equipos terminales móviles

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

- 4.1. Las empresas operadoras de servicios públicos móviles están obligadas a bloquear de manera inmediata el código IMEI (International Mobile Equipment Identity) y la línea asociada de los equipos terminales móviles que sean reportados como sustraídos o perdidos por el abonado, su representante o el usuario, conforme al Reglamento del Decreto Legislativo 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana. El bloqueo impedirá el uso del equipo en cualquier red nacional e internacional.
- 4.2. Los fabricantes de equipos terminales móviles que comercialicen dispositivos en el país deben incorporar funciones nativas de bloqueo remoto y borrado seguro ("kill switch") que permitan al usuario desactivar el equipo en caso de sustracción o pérdida. El MTC y el OSIPTEL establecen los requisitos técnicos mínimos y la forma de activación de estas funciones.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación

El Poder Ejecutivo reglamenta la presente ley en un plazo de noventa días hábiles contados desde su entrada en vigor, estableciendo los procedimientos y las condiciones técnicas para su aplicación.

SEGUNDA. Financiamiento

La implementación de lo dispuesto en la presente ley se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al tesoro público.

TERCERA. Coordinación intersectorial

El Ministerio de Transportes y Comunicaciones, el Ministerio del Interior, el Ministerio de Justicia y Derechos Humanos y el OSIPTEL, en el marco de sus competencias, coordinan acciones para prevenir la comercialización ilegal de equipos terminales móviles y fortalecer la confianza digital. Las coordinaciones incluyen la conformación de un grupo de trabajo permanente con participación del sector privado y de organizaciones de usuarios.

DISPOSICIÓN COMPLEMENTARIA MODIFICATORIA

ÚNICA. Modificación de los artículos 6 y 8 del Decreto Legislativo 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana

Se modifican el párrafo 6.3 del artículo 6 y el párrafo 8.1 del artículo 8 del Decreto Legislativo 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana, en los siguientes términos:

DICTAMEN POR MAYORÍA RECAÍDO EN EL PROYECTO DE LEY 4247/2022-CR, LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MÓVILES

"Artículo 6. Autoridades competentes

6.1 [...]

[...]

6.3 **El Ministerio Público, la Policía Nacional del Perú y el Poder Judicial, en el marco de la investigación de un delito y previa autorización judicial, acceden a la información contenida en el RENTSEGE a través de la Plataforma de Interoperabilidad del Estado (PIDE), conforme a la regulación vigente en materia de gobierno digital.**

6.4 [...]

Artículo 8. Empresas operadoras de servicios públicos de telecomunicaciones

8.1 Las empresas operadoras de servicios públicos móviles de telecomunicaciones tienen las siguientes obligaciones:

- a) Verificar plenamente la identidad de quien contrata el servicio de servicios públicos móviles de telecomunicaciones mediante **sistemas biométricos de huella dactilar u otras tecnologías de autenticación que ofrezcan niveles de seguridad equivalentes y que cuenten con la evaluación técnica y autorización del Ministerio de Transportes y Comunicaciones y del OSIPTEL**".

Dase cuenta

Sala de Comisión

Lima, 16 de marzo de 2026.



Firmado digitalmente por:
MORI CELIS Juan Carlos
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 17/03/2026 12:56:35-0500



Firmado digitalmente por:
PAREDES FONSECA Karol
Ivett FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 17/03/2026 15:30:27-0500



Firmado digitalmente por:
ACUÑA PERALTA Segundo
Hector FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 17/03/2026 15:57:33-0500



Firmado digitalmente por:
PAZO NUNURA Jose Bernardo
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 18/03/2026 11:13:50-0500



Firmado digitalmente por:
PICON QUERO Luis Raul FAU
20161749126 soft
Motivo: Soy el autor del documento
Fecha: 18/03/2026 12:47:27-0500



Firmado digitalmente por:
FLORES ANCACHI Jorge Luis
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 17/03/2026 16:46:45-0500



Firmado digitalmente por:
PARIONA SINCHE Alfredo
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 19/03/2026 11:30:39-0500



Firmado digitalmente por:
PAREDES FONSECA Karol
Ivett FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 20/03/2026 16:10:58-0500



Firmado digitalmente por:
QUISPE MAMANI Wilson
Rusbel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 19/03/2026 15:09:27-0500



Firmado digitalmente por:
TAPE CORONADO Maria
Elizabeth FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 19/03/2026 12:04:52-0500



Firmado digitalmente por:
ZEA CHOQUECHAMBI Oscar
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 18/03/2026 15:30:25-0500



Firmado digitalmente por:
VALER PINTO Hector FAU
20161749126 soft
Motivo: Soy el autor del documento
Fecha: 20/03/2026 14:01:16-0500