REPORTE TEMÁTICO N° 181/2024-2025-ASISP/DIP

Delitos informáticos
Legislación nacional

Lima, 3 de junio de 2025

PRESENTACIÓN

El Departamento de Investigación Parlamentaria, a través del Área de Servicios de Investigación y Seguimiento Presupuestal, ha elaborado el Reporte Temático N° 181 /2024-2025-ASISP/DIP, referido al ordenamiento jurídico vigente sobre los delitos informáticos.

Para la elaboración se ha consultado la información disponible en fuentes oficiales sobre la materia; cuyas referencias se consignan en el documento.

Esperamos brindar información que contribuya a la labor parlamentaria

I. Alcances generales

1. El Ministerio de Justicia de la República Argentina, menciona los conceptos y formas del ciberdelito[1]:

> Son conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas.
>
> Consiste en estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como *cyberbulling*, *grooming*, *phishing* cometidos por ciberdelincuentes que actúan en grupos o trabajan solos.
>
> *¿Qué es el ciberespacio?*
> Es un área intangible a la que cualquier persona puede acceder con una computadora desde su hogar, su lugar de trabajo o dispositivos móviles.
>
> *¿Qué medios usan los ciberdelincuentes para cometer un ciberdelito?*
> Usan medios tecnológicos como: internet, computadoras, celulares, redes de comunicación 3G, 4G y 5G, redes de fibra óptica y *software*.
>
> *¿Cómo es más probable que se tope con el ciberdelito un usuario cotidiano de equipos y dispositivos móviles?*
> El ciberdelito puede llegar de muchas maneras: sitios web no seguros, redes sociales, agujeros creados por vulnerabilidades de seguridad, contraseñas poco seguras en cuentas y dispositivos inteligentes y, sobre todo, el correo electrónico.
>
> *¿Cuáles son los ciberdelitos y contravenciones más comunes?*
> Los ciberdelitos se cometen a través de programas maliciosos desarrollados para borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin tu autorización y con fines económicos y de daño.
>
> Algunos ejemplos son:
>
> - **Ataques en tu navegación:** desvían tu navegador hacia páginas que causan infecciones con programas malignos como virus, gusanos y troyanos. Estos programas pueden borrar tu sistema operativo, infectar tu teléfono y tu computadora, activar tu webcam, extraer datos, etc.
> - **Ataques a servidores:** pueden dañar o robar tus datos y negarte el acceso a tu información.
> - **Corrupción de bases de datos**: interfieren en bases de datos públicas o privadas para generar datos falsos o robar información.
> - **Virus informáticos:** encriptan archivos, bloquean cerraduras inteligentes, roban dinero desde los celulares con mensajes de texto que parecen de la compañía.
> - **Programa espía:** alguno de los dispositivos tiene instalado un *software* que le permite encender y grabar con la cámara y el micrófono. También puede acceder a tu información personal sin autorización y sin que lo sepas.
>
> Los ciberdelitos usan la ingeniería social para engañarte, amenazarte y sacarte datos personales o información de otras personas u organizaciones, obtener dinero, suplantar tu identidad, acosarte digital y sexualmente.
>
> Algunos ejemplos son:
>
> - ***Phishing*** o ***vishing:*** los ciberdelincuentes se hacen pasar por empresas de servicios, oficinas de gobierno o amigos de algún familiar y te piden los datos
>
>   que les faltan para suplantar tu identidad y así operar tus cuentas en bancos, perfiles en las plataformas y redes sociales, servicios y aplicaciones web.

[1] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

- ***Ciberbullying:*** es el acoso por mensajería instantánea, *stalking* en WhatsApp, Telegram, Facebook Messenger y en las redes sociales con la intención de perseguir, acechar, difamar y atentar contra el honor e integridad moral de una persona. Esto lo hacen a través del descubrimiento y revelación de secretos, de la publicación de comentarios o videos ofensivos o discriminatorios, de la creación de memes o el etiquetado de tus publicaciones.

- ***Grooming:*** se trata de personas adultas que, de manera velada, intentan obtener fotografías o videos sexuales de personas menores para posteriores chantajes o previo al abuso sexual.

- **Sextorsión:** consiste en pedir dinero a cambio de no difundir en las redes imágenes generadas para un intercambio erótico consentido.

- **Ciberodio:** son contenidos inapropiados que pueden vulnerar a las personas. Se considera ciberodio a la violencia, mensajes que incitan al odio, la xenofobia, el racismo y la discriminación o el maltrato animal.

- **Pornografía infantil:** se trata de la corrupción de personas menores y su explotación sexual para producir, comercializar imágenes y videos de actividad sexual explícita.

Uso de la **inteligencia artificial** en ciberdelitos
Los ciberdelincuentes utilizan la IA para hacer sus ataques más sofisticados y difíciles de detectar. Algunas de las formas de amenazas más frecuentes son :

Phishing **personalizado:** la IA analiza datos de redes sociales para crear correos electrónicos de phishing muy convincentes, dirigidos a individuos específicos.

***Deepfakes* y suplantación de identidad:** Los deepfakes son vídeos, imágenes o archivos de voz manipulados con software de inteligencia artificial (IA) para parecer reales y auténticos. Los ciberdelincuentes pueden usarlos para extorsionar, cometer fraude o manipular a las víctimas para que realicen acciones perjudiciales.

Malware Inteligente: el malware impulsado por IA puede adaptarse y evitar ser detectado por los sistemas de seguridad tradicionales.

Exploración de Vulnerabilidades: la IA puede detectar rápidamente fallos en el software y las redes, que los atacantes pueden explotar antes de que se solucionen.

Otra dimensión del ciberdelito tiene que ver con la violación de la privacidad de las personas

- Espionaje ilícito sobre las comunicaciones privadas de los ciudadanos.

- Violación a la intimidad por parte de las empresas proveedoras de servicios de internet sin el consentimiento del usuario, para conocer sus gustos y preferencias y establecer la venta agresiva de productos y servicios asociados.

- Acceso ilegal a las comunicaciones privadas de un trabajador (correos electrónicos, redes sociales, etc.)

2. La Organización International de Policía Criminal (INTERPOL) describe el fenómeno de la ciberdelincuencia y lo clasifica en los términos siguientes[2]:

> Hoy en día, el mundo está más conectado digitalmente que nunca. Los delincuentes se están aprovechando de esta transformación en línea para atacar, a través de sus puntos débiles, las redes, infraestructuras y sistemas informáticos. Esto tiene una enorme repercusión económica y social en todo el mundo, tanto para los gobiernos, como para las empresas o los particulares.
>
> El phishing, el ransomware y las violaciones de la seguridad de los datos son solo algunos ejemplos de las actuales ciberamenazas, eso sin contar que continuamente están surgiendo nuevos tipos de ciberdelitos. Los ciberdelincuentes son cada vez más ágiles y están mejor organizados, como demuestra la velocidad con que explotan las nuevas tecnologías, y el modo en que adaptan sus ataques y cooperan entre sí de forma novedosa.
>
> Los ciberdelitos no conocen fronteras. Los delincuentes, las víctimas y las infraestructuras técnicas están dispersos por múltiples jurisdicciones, lo que resulta muy problemático a la hora de realizar una investigación o emprender acciones judiciales.
>
> (…)

3. El Proyecto #CREW, financiado con el apoyo de la Comisión Europea, brinda una definición de piratería y extorsión cibernética[3]:

> La piratería (“Hacking”) es un intento de explotar un sistema informático o una red privada dentro de un ordenador. En pocas palabras, es el acceso no autorizado o el control de los sistemas de seguridad de la red informática para algún propósito ilícito.
>
> La extorsión cibernética es un delito en Internet en el que alguien retiene archivos electrónicos o los datos de su empresa como rehenes hasta que se les pague el rescate exigido.

[2] https://www.interpol.int/es/Delitos/Ciberdelincuencia

[3] https://crewproject.eu/hacking-y-extorsion-cibernetica/

CUADRO 1

OBJETIVO DE LAS PRINCIPALES NORMAS QUE REGULAN LOS DELITOS INFORMÁTICOS EN EL PERÚ

Constitución Política	Ley 30096 Ley de Delitos Informáticos	Ley 30999 Ley de Ciberdefensa	Ley 29733 Ley de Protección de Datos personales	Ley 30077 Ley Contra el Crimen Organizado	Decreto Legislativo N.º 1412 Decreto Legislativo que aprueba la Ley de Gobierno Digital	Decreto Supremo N.º 010-2019-RE Convenio sobre la Ciberdelincuencia	Resolución de la Fiscalía de la Nación N.º 2893-2024-MP-FN
Toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.	Tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.	Tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.	Tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en la Constitución Política, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.	Fija las reglas y procedimientos relativos a la investigación, juzgamiento y sanción de los delitos cometidos por organizaciones criminales.	El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.	El objetivo principal del Convenio es instaurar una política penal común para resguardar a la sociedad contra la ciberdelincuencia, fomentando la cooperación internacional y la adopción de legislaciones adecuadas.	De Acuerdo a la presente resolución se dispone que el delito de préstamos informáticos extorsivos previsto en el artículo 8-A de la Ley N° 30096, en atención a su naturaleza será de competencia de las fiscalías provinciales penales y/o mixtas y amplían competencia material de las Fiscalías Especializadas contra la Criminalidad Organizada

Fuente: SPIJ. Elaboración: Área de Servicios de Información y Seguimiento Presupuestal (ASISP)

CUADRO 2

LEGISLACIÓN NACIONAL

Norma	Artículo
Constitución Política del Perú	**Artículo 2.** Toda persona tiene derecho: (…). 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. 7. Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley. **Artículo 44**. Son deberes primordiales del Estado: defender la soberanía nacional; garantizar la plena vigencia de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación. (…).
Ley 30096 Ley de Delitos Informáticos	**Artículo 1. Objeto de la Ley** La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. **Artículo 2. Acceso ilícito** El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa. **Artículo 3. Atentado a la integridad de datos informáticos** El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa. **Artículo 4. Atentado a la integridad de sistemas informáticos** El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

	Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de seis ni mayor de nueve años. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años. En todos los casos se impone, además, la pena de inhabilitación conforme a los numerales 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11 del artículo 36 del Código Penal. **Artículo 5-A.- Chantaje sexual con materiales elaborados o modificados por medios digitales o tecnológicos** El que, mediante el uso de tecnologías de la información o comunicación, amenaza o intimida a una persona, con la difusión de imágenes, materiales audiovisuales o audios elaborados o modificados por medios digitales o tecnológicos, para obtener de ella una conducta o acto de connotación sexual, será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años e inhabilitación, según corresponda, conforme a los incisos 5, 9, 10 y 11 del artículo 36 del Código Penal. La pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitación, cuando concurra cualquiera de las siguientes circunstancias: 1. La amenaza a la víctima se refiere a la difusión de imágenes, materiales audiovisuales o audios con contenido sexual en los que esta aparece o participa. 2. Cuando la víctima mantenga o haya mantenido una relación de pareja con el agente, son o han sido convivientes o cónyuges. 3. Cuando la víctima es menor de 18 años de edad. **Artículo 6 (Derogado)** **Artículo 7. Interceptación de datos informáticos** El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública. La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores. **Artículo 8. Fraude informático**

	El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos. **Artículo 8-A. Préstamos informáticos extorsivos** El que, a través de plataformas digitales, internet u otro medio análogo induce u obliga mediante amenaza, intimidación, engaño o ardid a aceptar dinero o bienes, simulando un contrato de mutuo o cualquier otro con el fin de obtener una ventaja indebida, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años. La pena será no menor de quince ni mayor de veinticinco años, cuando: a) Se ejerce violencia para obtener la ventaja indebida. b) La víctima tiene discapacidad, tiene entre catorce y menos de dieciocho años de edad o es adulta mayor, padece de una enfermedad grave, pertenece a un pueblo indígena u originario, o presenta cualquier situación de vulnerabilidad. c) El agente comete el delito en el marco de la actividad de una persona jurídica. d) La comisión del hecho punible es de carácter transnacional, de acuerdo al numeral 2 del artículo 3 de la Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional - Convención de Palermo **Artículo 9. Suplantación de identidad** El que, mediante las tecnologías digitales suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral o de cualquier otra índole, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole. **Artículo 10. Abuso de mecanismos y dispositivos informáticos** El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. **Artículo 11. Agravantes** El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

	1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. 3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia. 4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales. **Artículo 12. Exención de responsabilidad penal** Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos. DISPOSICIONES COMPLEMENTARIAS FINALES **PRIMERA. Codificación de la pornografía infantil** La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada. La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior. **SEGUNDA. Agente encubierto en delitos informáticos** El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, **incluso si estas acciones deben realizarse en entornos digitales,** y con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957. Los protocolos para la actuación del agente encubierto en entornos digitales, tanto en el marco de la presente Ley, como en el marco del artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957, son coordinados, en cuanto corresponda, con la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en concordancia con las normas vigentes que regulan el Sistema Nacional de Transformación Digital. **TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados** La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad. **CUARTA. Cooperación operativa**

	Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley. **QUINTA. Capacitación** Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial- en el tratamiento de los delitos previstos en la presente Ley. **SEXTA. Medidas de seguridad** La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos. **SÉTIMA. Buenas prácticas** El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas. **OCTAVA. Convenios multilaterales** El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos. **NOVENA. Terminología** Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001: a. **Por sistema informático:** todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. b. **Por datos informáticos:** toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. **DÉCIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP** La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957. El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

	UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957. Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal. El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente. (…)
Ley 30999 Ley de Ciberdefensa	TÍTULO I DISPOSICIONES GENERALES **Artículo 1. Objeto** La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley. **Artículo 2. Finalidad** Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional. **Artículo 3. Ámbito de aplicación** El ámbito de aplicación de la norma se circunscribe a la ejecución de operaciones de ciberdefensa en y mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional. **Artículo 4. Definición** Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional. **Artículo 5. Órganos ejecutores** Las Fuerzas Armadas, que están constituidas por el Ejército, la Marina de Guerra y la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa. TÍTULO II DE LA CIBERDEFENSA CAPÍTULO I LAS CAPACIDADES DE CIBERDEFENSA Y LAS OPERACIONES EN Y MEDIANTE EL CIBERESPACIO

	Artículo 6. De las capacidades de ciberdefensa Es el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias. **Artículo 7. De las operaciones militares en el ciberespacio** Es el eficiente y eficaz empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo a sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o los ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional. **Artículo 8. De la planificación y ejecución de las operaciones en el ciberespacio** La planificación y ejecución de las operaciones de ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la presente ley, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables. CAPÍTULO II DEL USO DE LA FUERZA EN Y MEDIANTE EL CIBERESPACIO **Artículo 9. Del uso de la fuerza por las Fuerzas Armadas** El uso de la fuerza por la Fuerzas Armadas en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y el presente dispositivo legal, y está regido por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario que sean aplicables. **Artículo 10. De la legítima defensa** Toda amenaza o ataque en y mediante el ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al ejercicio del derecho de legítima defensa. **Artículo 11. Requisitos para el ejercicio del uso de la fuerza** El ejercicio del derecho de legítima defensa en el contexto de las operaciones de ciberdefensa está sujeto a los principios de legalidad, necesidad y oportunidad. En el caso de conducir una operación de respuesta en y mediante el ciberespacio que contenga un ataque deliberado, debe realizarse de acuerdo a ley. CAPÍTULO III DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES **Artículo 12. Del control y de la protección de los activos críticos nacionales y recursos claves** El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

	Artículo 13. De los protocolos de escalamiento, coordinación, intercambio y activación La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la presente ley. Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Informática y de la seguridad digital en el país, quien emite los lineamientos y las directivas correspondientes. (…).
Ley 29733 Ley de Protección de Datos personales	TÍTULO PRELIMINAR DISPOSICIONES GENERALES **Artículo 1. Objeto de la Ley** La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. (…). TÍTULO II TRATAMIENTO DE DATOS PERSONALES **Artículo 13. Alcances sobre el tratamiento de datos personales** 13.1 El tratamiento de datos personales debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y de los derechos que esta Ley les confiere. Igual regla rige para su utilización por terceros. 13.2 Las limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, respetando su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos. 13.3 Mediante reglamento se dictan medidas especiales para el tratamiento de los datos personales de los niños y de los adolescentes, así como para la protección y garantía de sus derechos. Para el ejercicio de los derechos que esta Ley reconoce, los niños y los adolescentes actúan a través de sus representantes legales, pudiendo el reglamento determinar las excepciones aplicables, de ser el caso, teniendo en cuenta para ello el interés superior del niño y del adolescente. 13.4 Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los datos personales obtenidos con violación de este precepto carecen de efecto legal. 13.5 Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco.

	13.6 En el caso de datos sensibles, el consentimiento para efectos de su tratamiento, además, debe efectuarse por escrito. Aun cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público. 13.7 El titular de datos personales puede revocar su consentimiento en cualquier momento, observando al efecto los mismos requisitos que con ocasión de su otorgamiento. 13.8 El tratamiento de datos personales relativos a la comisión de infracciones penales o administrativas solo puede ser efectuado por las entidades públicas competentes, salvo convenio de encargo de gestión conforme a la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. Cuando se haya producido la cancelación de los antecedentes penales, judiciales, policiales y administrativos, estos datos no pueden ser suministrados salvo que sean requeridos por el Poder Judicial o el Ministerio Público, conforme a ley. 13.9 La comercialización de datos personales contenidos o destinados a ser contenidos en bancos de datos personales se sujeta a los principios previstos en la presente Ley. **Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales** No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos: 1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias. 2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público. 3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley. 4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario. 5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento. 6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.

	7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos. 8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación. 9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales. 10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal. 11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada. 12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información. 13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley. (…). **Artículo 16. Seguridad del tratamiento de datos personales** Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes. Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo. (…).
Ley 30077 Ley Contra el Crimen Organizado	**Artículo 1. Objeto de la Ley** La presente Ley tiene por objeto fijar las reglas y procedimientos relativos a la investigación, juzgamiento y sanción de los delitos cometidos por organizaciones criminales. **Artículo 2. Definición y criterios para determinar la existencia de una organización criminal** 2.1. Para efectos de la presente ley, se consideran las siguientes definiciones:

	a) Organización criminal. Se considera organización criminal a todo grupo con compleja estructura desarrollada y mayor capacidad operativa compuesto por tres o más personas con carácter permanente o por tiempo indefinido que, de manera concertada y coordinada, se reparten roles correlacionados entre sí, para la comisión de delitos de extorsión, secuestro, sicariato y otros delitos sancionados con pena privativa de libertad igual o mayor de cinco años en su extremo mínimo, con el fin de obtener, directa o indirectamente, un beneficio económico u otro de orden material. b) Grupo con estructura desarrollada. Es el grupo de tres o más personas que no ha sido constituido fortuitamente y en el que necesariamente sus miembros tienen determinados roles y correlacionados entre sí, que logran de esa manera su permanencia en el tiempo e integración en la organización. c) Capacidad operativa. Suma de medios y recursos idóneos, de hecho o de derecho, para el desarrollo del programa criminal. d) Delito grave. Son aquellos delitos sancionados con pena privativa de libertad mayor de seis años. 2.2. La comisión del hecho punible se materializa con la concurrencia de un grupo con compleja estructura desarrollada y con mayor capacidad operativa, potencialmente capaz de llevar a cabo un programa criminal. **Artículo 3.- Delitos comprendidos** La presente Ley es aplicable a los siguientes delitos: (…). 8. Delitos informáticos previstos en la ley penal. (…).
Decreto Legislativo N.º 1412 Decreto Legislativo que aprueba la Ley de Gobierno Digital	SEGURIDAD DIGITAL **Artículo 30.- De la Seguridad Digital** La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas. **Artículo 31.- Marco de Seguridad Digital del Estado Peruano** El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública. **Artículo 32.- Gestión del Marco de Seguridad Digital del Estado Peruano** El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos: **a. Defensa:** El Ministerio de Defensa (MINDEF), en el marco de sus funciones y competencias, dirige, norma, supervisa y evalúa las normas en materia de ciberdefensa.

	b. Inteligencia: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia. **c. Justicia:** El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia. **d. Institucional:** Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI). **Artículo 33.- Articulación de la Seguridad Digital con la Seguridad de la Información** El Marco de Seguridad Digital del Estado Peruano se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.
Decreto Supremo N.º 010-2019-RE Ratifican el "Convenio sobre la Ciberdelincuencia"	**Artículo 1.-** Ratifícase el "Convenio sobre la Ciberdelincuencia"[4] adoptado el 23 de noviembre de 2001 en la ciudad de Budapest, Hungría, y aprobado por Resolución Legislativa Nº 30913, de 12 de febrero de 2019, con las siguientes declaraciones y reservas: **DECLARACIONES** a) De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad. b) De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático. c) De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal. d) De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el literal e) del numeral 9 del citado artículo del Convenio deberán dirigirse a su autoridad central.

[4] Convenio sobre la Ciberdelincuencia. Ver texto completo: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1244293

	RESERVAS a) De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio. b) De conformidad con el numeral 4 del artículo 9 del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad. c) Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal. **Artículo 2.-** De conformidad con los artículos 4 y 6 de la Ley Nº 26647, el Ministerio de Relaciones Exteriores procederá a publicar en el diario oficial “El Peruano” el texto íntegro del tratado, así como su fecha de entrada en vigencia.
Resolución de la Fiscalía de la Nación N.º 2893-2024-MP-FN	**MINISTERIO PÚBLICO** **Disponen que el delito de préstamos informáticos extorsivos previsto en el artículo 8-A de la Ley N° 30096, en atención a su naturaleza será de competencia de las fiscalías provinciales penales y/o mixtas y amplían competencia material de las Fiscalías Especializadas contra la Criminalidad Organizada** (…). SE RESUELVE: **Artículo Primero. -** Disponer que el delito de préstamos informáticos extorsivos previsto en el artículo 8-A de la Ley N.°30096 -incorporado mediante la Ley N° 32183-, en atención a su naturaleza será de competencia de las fiscalías provinciales penales y/o mixtas. **Artículo Segundo. -** Ampliar a partir del día siguiente de la publicación del presente acto resolutivo, la competencia material de las Fiscalías Especializadas contra la Criminalidad Organizada, para conocer el delito al que se refiere el artículo precedente, siempre y cuando se cometa en el contexto de una organización o banda criminal. **Artículo Tercero.-** Disponer la notificación de la presente resolución al Ministerio del Interior, Primera Fiscalía Suprema en lo Penal, Segunda Fiscalía Suprema en lo Penal, Fiscalía Suprema de Familia, Fiscalía Suprema Especializada en Delitos Cometidos por Funcionarios Públicos, Primera Fiscalía Suprema Transitoria Especializada en Delitos Cometidos por Funcionarios Públicos, Segunda Fiscalía Suprema Transitoria Especializada en Delitos Cometidos por Funcionarios Públicos, Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y Coordinación Nacional de las Fiscalías Especializadas en Ciberdelincuencia, Coordinación Nacional de las Fiscalías Especializadas contra la Criminalidad Organizada, Presidencias de las Junta de Fiscales Superiores a nivel nacional, Oficina de Registro y Evaluación de Fiscales, Oficina de Productividad Fiscal, Oficina

	Técnica de Implementación del Nuevo Código Procesal Penal, Secretaría General de la Fiscalía de la Nación, Gerencia General y Oficina de Imagen Institucional, para los fines pertinentes.

Fuente: Constitución Política del Perú. Sistema Peruano de Información Jurídica (SPIJ)
Elaboración: Área de Servicios de Información y Seguimiento Presupuestal (ASISP)