REPORTE

GPS

La otra cara de la conexión:

la ciberdelincuencia en el Perú

2020 - 2026



Noviembre, 2026

La otra cara de la conexión: - la ciberdelincuencia en el Perú, 2020–2026
Elaboración: Cecilia Caparachín

Responsables
Cecilia Caparachin - Directora de Investigación
Benjamín Durand - Investigador
Ximena Montenegro - Investigadora

Dirección de Marketing y Comunicaciones
Katia Olivares

Publicado por:
GPS Agencia
Lima, Perú
www.gpsagencia.com

ÍNDICE

- **Un país cada vez más conectado..... 03**
- **¿Qué dice la ley sobre los delitos informáticos?..... 06**
- **Una tendencia en aumento: las denuncias entre 2020 y 2026..... 09**
- **Dos delitos concentran casi nueve de cada diez denuncias..... 10**
  - Fraude informático: cuando el objetivo es tu dinero..... 11
  - Suplantación de identidad: cuando alguien se hace pasar por ti... 13
- **¿Dónde se denuncia más?..... 14**
- **Conclusiones..... 18**
- **¿Cómo evitar ser víctima de un delito informático?..... 20**
  - Para prevenir el fraude informático..... 20
  - Para prevenir la suplantación de identidad..... 21
- **Nota metodológica..... 22**
- **Referencias..... 23**

Puntos clave:

8 de cada diez peruanas y peruanos de 12 años a más usan internet, y casi todos se conectan desde el celular.



Las denuncias por delitos informáticos se multiplicaron casi por cinco: pasaron de **8,674** **en 2020 a** **42,980** **en 2025.**

En 2026 la tendencia se acelera:

39,307 denuncias entre enero y setiembre unas **144** por día y **18.5%** más que en el mismo periodo de 2025.

Dos delitos explican casi nueve de cada diez denuncias por delitos informáticos: el fraude informático **(67.5%)** y la suplantación de identidad (21.8%).



Los cuatro distritos fiscales de Lima con más casos concentran más de la mitad de las denuncias, pero el crecimiento más rápido se da en distritos fiscales como: **Ayacucho, Sullana, Apurímac, Tumbes y Madre de Dios.**

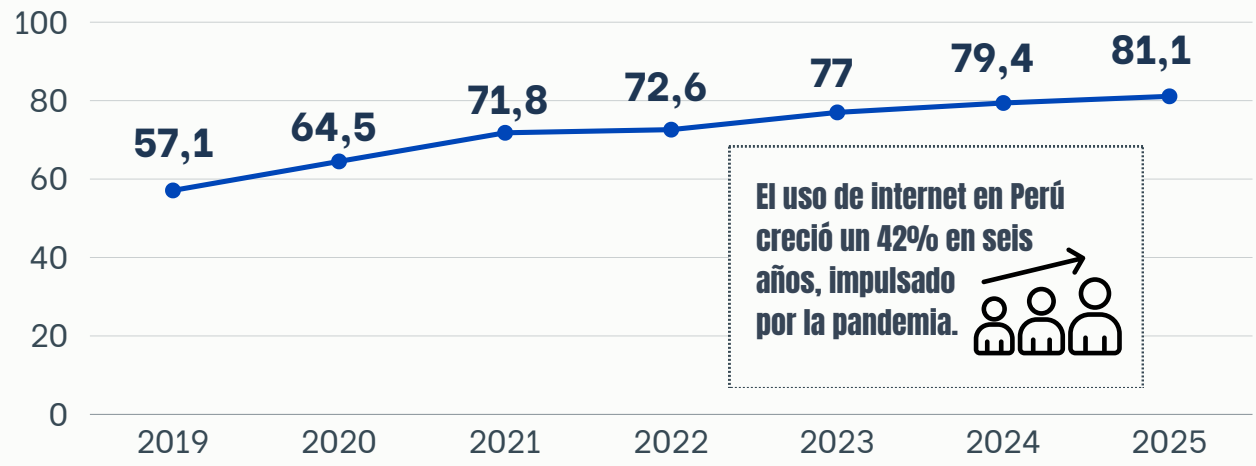


1.Un país cada vez más conectado



En las últimas décadas, el desarrollo tecnológico ha puesto al alcance de las personas herramientas que facilitan muchos aspectos de la vida diaria: comunicarse, informarse, estudiar, comprar o pagar. Internet, en particular, ha acortado distancias. El Perú no ha sido ajeno a este proceso y el uso de internet se ha vuelto casi universal. En 2025, ocho de cada diez peruanas y peruanos de 12 años a más (81.1%) usaron internet, frente a 57.1% en 2019. Es decir, la proporción de usuarios creció 42% en seis años, con un salto especialmente marcado durante la pandemia.

Gráfico 1. Perú: población de 12 y más años de edad que usó internet el mes anterior, 2019-2025 (%)



El celular, la principal puerta de entrada a internet

El celular es la principal puerta de entrada a internet. Casi todas las personas usuarias (94.3%) se conectan desde un teléfono móvil, muy por encima de quienes lo hacen desde su hogar (28.2%), el trabajo (7.9%) o un centro educativo (4.0%). En la práctica, buena parte de la vida digital, y también de sus riesgos, cabe en un bolsillo.





Nota: respuesta múltiple; una persona puede conectarse desde más de un lugar.
Fuente: Instituto Nacional de Estadística e Informática (INEI, 2026), Encuesta Nacional de Hogares (ENAHO). Elaboración propia.

¿Para qué se usa internet?

Internet se usa sobre todo para comunicarse (92.5%), entretenerse (91.9%) e informarse (78.3%). Además, más de la tercera parte de las personas usuarias (37.9%) lo emplea para la banca electrónica y otras operaciones financieras, y 15% lo usa para comprar. Cada una de estas actividades supone compartir datos personales, claves o dinero a través de la red.

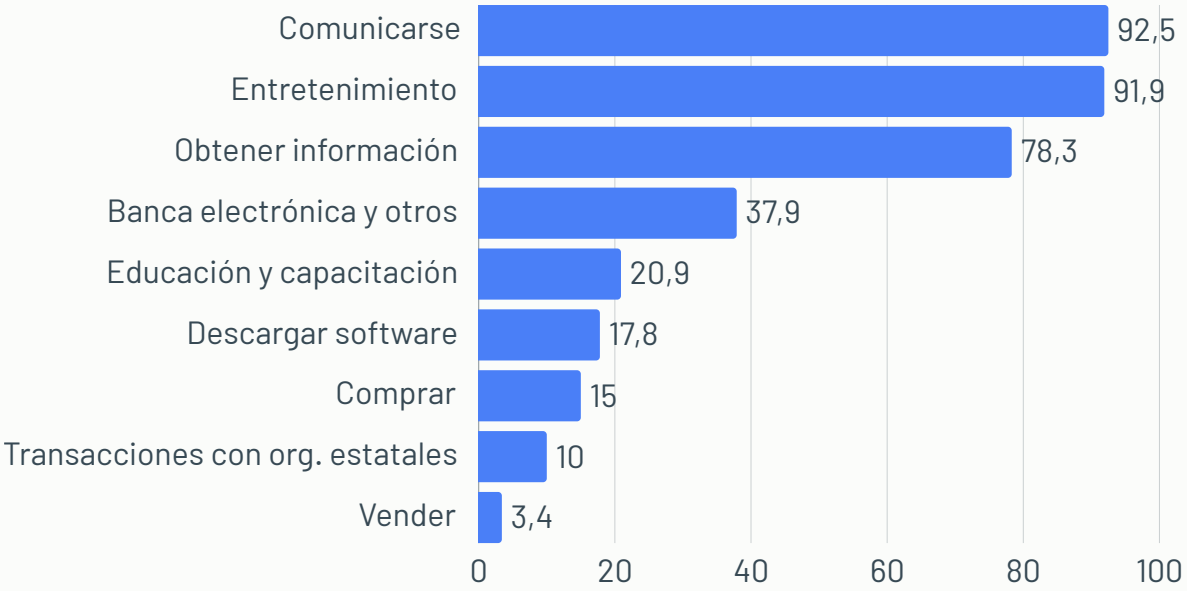
92,5% Comunicarse

91,9% Entretenerse

78,3% Informarse

37,9% Banca electrónica y otras operaciones financieras

15% Comprar



Nota: respuesta múltiple; una persona puede usarlo para más de una actividad.
Fuente: Instituto Nacional de Estadística e Informática (INEI, 2026), Encuesta Nacional de Hogares (ENAHO). Elaboración propia.

En este panorama de uso casi masivo existe también un riesgo creciente: la ciberdelincuencia. Así como hay delitos que se cometen en la calle, en el mundo digital hay personas que aprovechan la tecnología para robar dinero, apropiarse de identidades ajenas o dañar información y sistemas. Este reporte describe qué dice la ley peruana sobre estos delitos, cómo han evolucionado las denuncias entre 2020 y 2026 y dónde se concentran.

Cada una de estas actividades supone **compartir datos personales,** claves o dinero a través de la red.

2. ¿Qué dice la ley sobre los delitos informáticos?

En el Perú, los delitos informáticos están regulados principalmente por la Ley N.° 30096, Ley de Delitos Informáticos, publicada en octubre de 2013. Su finalidad es prevenir y sancionar las conductas que afectan los sistemas y datos informáticos, así como otros bienes protegidos por la ley penal (como el patrimonio, la intimidad o la identidad), cuando se cometen usando tecnologías de la información o de la comunicación (Ley N.° 30096, 2013, art. 1).

¿Qué es un delito informático?

Dicho de forma simple, es un delito que se comete usando la tecnología (una computadora, un celular, internet o una aplicación) o contra la tecnología misma (un sistema, una base de datos o una cuenta).



La ley ha sido modificada varias veces para responder a nuevas formas de delinquir. Entre los cambios más relevantes destacan:

2014	Ley N.° 30171: precisó la redacción de varios delitos.
2023	Decretos Legislativos N.° 1591 y N.° 1614: elevaron las penas del fraude informático, la suplantación de identidad y el contacto con menores de edad con fines sexuales, e incluyeron expresamente la suplantación de páginas web como forma de fraude.
2024	Decreto Legislativo N.° 1625: incorporó un delito vinculado a la difusión de contenido sexual por medios digitales.
2024	Ley N.° 32183: incorporó los préstamos informáticos extorsivos.
2025	Ley N.° 32314: agravó las penas cuando se usa inteligencia artificial.
2025	Ley N.° 32451: sancionó la activación de chips o líneas móviles sin consentimiento del titular.
2025	Decreto Legislativo N.° 1700: castigó la compra, posesión y venta ilegal de datos y bases de datos personales.

Además, desde 2019 el Perú forma parte del Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest), el principal tratado internacional en la materia. Este convenio, aprobado por el Congreso mediante la Resolución Legislativa N.° 30913 y vigente para el país desde el 1 de diciembre de 2019, facilita la cooperación entre Estados para investigar delitos que muchas veces se cometen desde otros países (Resolución Legislativa N.° 30913, 2019). La Tabla 1 resume los principales delitos que contempla hoy la ley.

Tabla 1. Principales delitos de la Ley N.° 30096, Ley de delitos informáticos

Artículo	Delito	¿En qué consiste?
Contra los datos y sistemas informáticos		
2	**Acceso ilícito**	Entrar sin permiso a una computadora, cuenta, red o sistema, o ir más allá de lo autorizado. La pena es mayor si para entrar se rompen las medidas de seguridad.
3	**Atentado contra la integridad de datos informáticos**	Borrar, dañar, alterar o bloquear información digital ajena.
4	**Atentado contra la integridad de sistemas informáticos**	Dejar inutilizable un sistema o impedir que funcione o que preste su servicio (por ejemplo, hacer caer una página web).
Contra niñas, niños y adolescentes y la libertad sexual		
5	**Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**	Contactar a una persona menor de edad por internet u otro medio digital para pedirle material sexual o proponerle actos sexuales (conocido como grooming).
5-A	**Difusión de contenido sexual por medios digitales**	Sanciona conductas relacionadas con la difusión de imágenes, videos o audios de contenido sexual mediante tecnologías digitales.
8	**Fraude informático**	Obtener un beneficio económico indebido, en perjuicio de otra persona, manipulando datos, sistemas o páginas web.
8-A	**Préstamos informáticos extorsivos**	Versión digital de los préstamos "gota a gota": usar plataformas o medios digitales para imponer préstamos o cobrarlos mediante amenazas o intimidación.

Contra la fe pública		
9	**Suplantación de identidad**	Hacerse pasar por otra persona o por una empresa usando medios digitales, causándole algún perjuicio.
9-A	**Activación de chip o línea móvil sin consentimiento**	Activar un chip (SIM) o una línea de celular a nombre de otra persona sin su autorización.
Disposiciones comunes		
10	**Abuso de mecanismos y dispositivos informáticos**	Fabricar, vender o facilitar programas, aparatos o contraseñas creados para cometer estos delitos.
11	**Agravantes**	La pena puede aumentar hasta en un tercio por encima del máximo cuando el delito lo comete una organización criminal; cuando alguien abusa de su cargo o de su acceso privilegiado a la información; cuando se busca un beneficio económico; cuando se comprometen fines asistenciales o la seguridad nacional; o cuando se usa inteligencia artificial.

Nota: el artículo 6 (tráfico ilegal de datos) fue derogado en 2014; esa conducta se sanciona en el artículo 154-A del Código Penal. Las descripciones son simplificadas y no reemplazan el texto legal.
Fuente: Ley N.° 30096 y sus modificatorias.
Elaboración propia.

3. Una tendencia en aumento: las denuncias entre 2020 y 2026

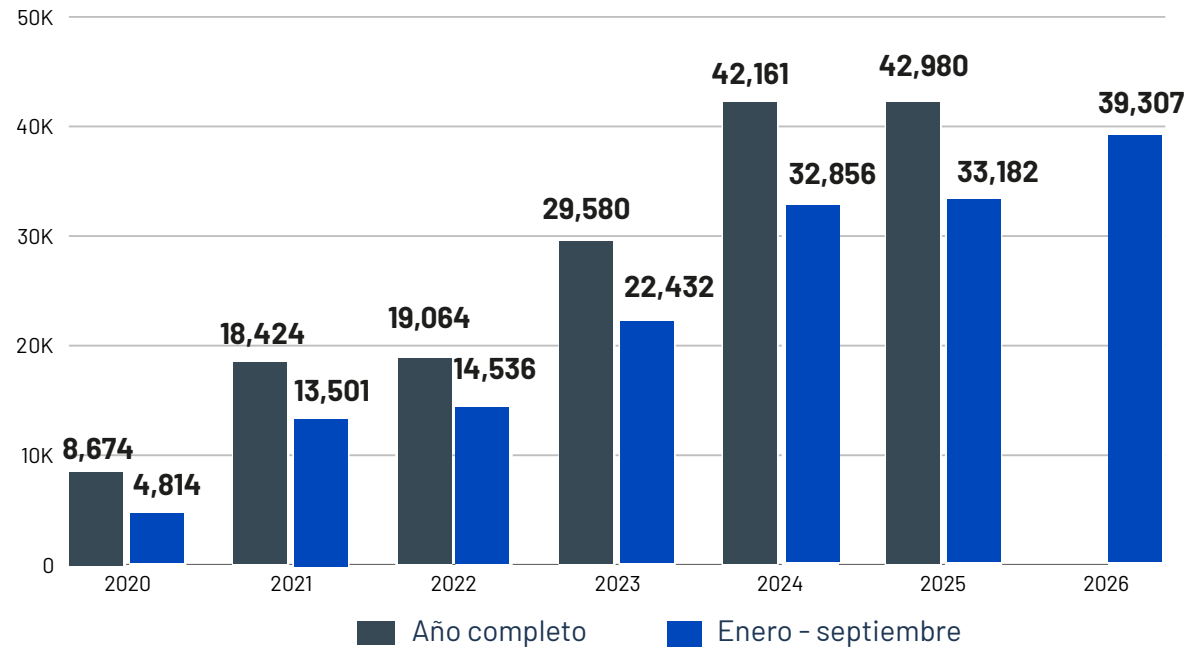
Según los registros del Ministerio Público, las denuncias por delitos informáticos han crecido de manera sostenida. En 2020 se registraron 8,674 denuncias; un año después la cifra ya se había duplicado (18,424), y en 2025 llegó a 42,980: casi cinco veces más que en 2020. El mayor salto se produjo entre 2023 y 2024 (+42.5%). En 2025 el número se mantuvo casi estable (+1.9%), pero 2026 muestra una nueva aceleración.

Entre enero y setiembre de 2026 se registraron 39,307 denuncias, 18.5% más que en los mismos meses de 2025 (33,182). Esto equivale, en promedio, a unas 144 denuncias por día o 6 denuncias cada hora. Con tres meses aún por registrar, 2026 ya alcanzó el 91% del total de 2025, por lo que es muy probable que cierre con la cifra más alta del periodo.

IMPORTANTE: una denuncia no es una condena

Las cifras de este reporte corresponden a denuncias registradas por el Ministerio Público. Una denuncia indica que un hecho fue puesto en conocimiento de la Fiscalía, pero no significa que el delito haya sido comprobado ni que exista un responsable identificado.
Además, no todas las víctimas denuncian. Por eso, el aumento de denuncias puede reflejar más delitos, pero también una mayor disposición a denunciar o mejoras en el registro. Las cifras deben leerse como una señal de tendencia y no como una medida exacta de cuántos delitos ocurren.

Gráfico 4. Denuncias por delitos informáticos, 2020-2026: año completo y enero-setiembre



Nota: las barras claras permiten comparar los mismos meses entre años.
Fuente: Ministerio Público – Fiscalía de la Nación, registro de denuncias por delitos informáticos 2020-2026 (enero-setiembre).
Elaboración propia.

4. Dos delitos concentran casi nueve de cada diez denuncias

Aunque la ley contempla más de una docena de delitos, dos concentran la gran mayoría de los casos. Entre 2020 y setiembre de 2026, el fraude informático representó 67.5% de todas las denuncias (135,169) y la suplantación de identidad, 21.8% (43,656). Juntos suman 89.3%. Ningún otro delito supera el 2% del total, y 5.3% de las denuncias no tiene registrado un delito específico.

Este peso, además, ha ido en aumento. En 2020 ambos delitos explicaban algo más de la mitad de las denuncias (56.2%); desde 2022 superan el 90%, y en 2025 alcanzaron 92.8%. En otras palabras, la ciberdelincuencia que se denuncia en el Perú está dirigida, sobre todo, contra el dinero y la identidad de las personas.

Principales delitos cibernéticos:

El fraude informático representa el 67.5% de los casos (135,169 denuncias),



La suplantación de identidad alcanza el 21.8% (43,656 denuncias).



Tendencia creciente

La ciberdelincuencia en el Perú está enfocada principalmente en el dinero y la identidad de las personas, lo que refleja una tendencia preocupante hacia la vulnerabilidad económica y personal.



Gráfico 5. Denuncias por delitos informáticos, según tipo de delito, 2020–2026 (% del total)



Fuente: Ministerio Público – Fiscalía de la Nación, registro de denuncias por delitos informáticos 2020–ene-set 2026.
Elaboración propia.

4.1. Fraude informático: cuando el objetivo es tu dinero

El fraude informático (artículo 8 de la Ley N.° 30096) ocurre cuando una persona, de manera deliberada, manipula, introduce, altera, borra o copia datos, suplanta una página web o interfiere en el funcionamiento de un sistema para obtener un beneficio indebido (por lo general, dinero) en perjuicio de otra persona o del Estado. En palabras simples: es usar la tecnología para apropiarse del dinero o de los bienes de otra persona sin su autorización.

La pena es de 4 a 8 años de cárcel, además de una multa. Sube a 5 a 10 años cuando se afecta el dinero del Estado destinado a fines asistenciales o a programas de apoyo social. La misma pena agravada alcanza a quien colabora a sabiendas facilitando la transferencia del dinero, como ocurre con las personas que prestan sus cuentas para recibir y mover los fondos robados (Decreto Legislativo N.° 1614, 2023).

Según la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional del Perú, las modalidades de fraude informático más denunciadas en el país son las siguientes (El Peruano, 2023):

Phishing:	Es la modalidad más denunciada. Los delincuentes copian la página web de un banco u otra entidad para engañar a las personas y obtener sus datos personales y claves. Luego suelen llamar a la víctima haciéndose pasar por el banco para pedirle el token que llega a su celular, y con esa información hacen transferencias sin su autorización.
Carding:	Uso ilegal de tarjetas bancarias ajenas para hacer compras por internet. Suelen empezar con compras pequeñas para no levantar sospechas.
SIM swapping	(duplicado de chip): con los datos personales de la víctima, el delincuente bloquea su chip y obtiene un duplicado a través de la empresa de telefonía. Así recibe los mensajes y códigos de la víctima, entra a su banca digital y hace transferencias o pide préstamos a su nombre.
Thief transfer	(fraude con celulares robados): los delincuentes sacan el chip de un celular robado o perdido, lo colocan en otro equipo y lo usan para acceder a la información y a las cuentas de la víctima.
Vishing	Llamadas telefónicas en las que el delincuente se hace pasar por una empresa, una entidad o una persona de confianza para obtener información personal y confidencial.
Uso de inteligencia artificial:	Videos falsos (deepfakes), voces clonadas u otras formas avanzadas de suplantación digital para engañar y obtener dinero. El Centro Nacional de Seguridad Digital ha emitido una alerta por el aumento de estafas que usan estas herramientas para fabricar rostros, voces y videos muy realistas (Infobae, 2026b).

La Policía Nacional también identifica entre los casos más frecuentes el robo de cuentas de WhatsApp mediante mensajes engañosos para obtener el código de verificación (El Peruano, 2025).

¿En qué se diferencia del delito de estafa?

El fraude informático suele confundirse con la estafa (artículo 196 del Código Penal). En la estafa, el delincuente engaña directamente a la víctima y es ella quien, convencida, entrega voluntariamente su dinero o sus bienes. En el fraude informático, en cambio, no siempre hay una interacción directa con la víctima: el delincuente ataca o manipula un sistema, una base de datos o un medio digital para sustraer el dinero o la información.

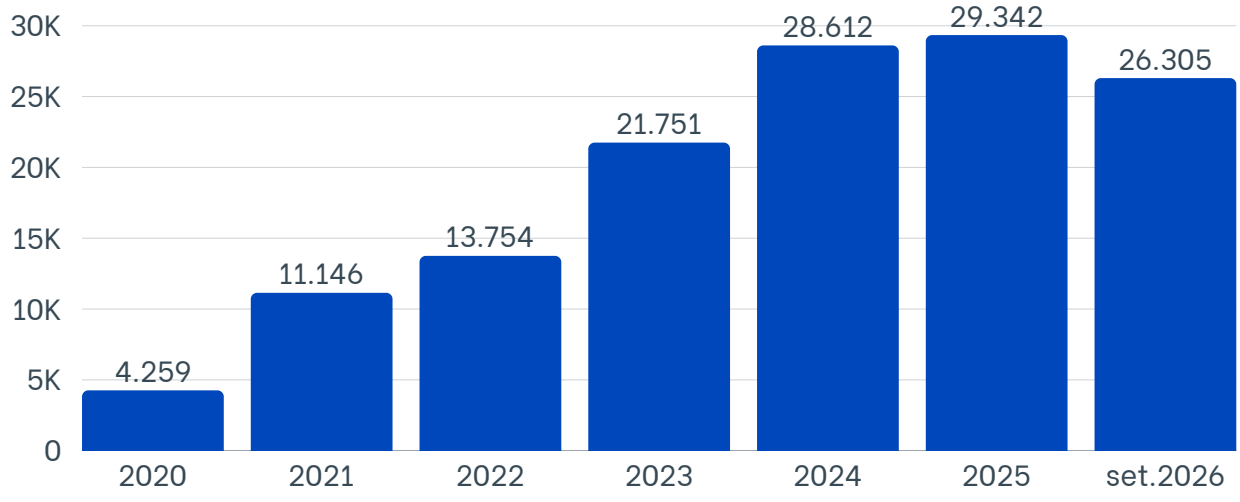
En la práctica, la línea entre ambos delitos no siempre es nítida, porque muchas modalidades combinan engaño y manipulación tecnológica. Por ejemplo, en las tiendas falsas la víctima paga voluntariamente, por lo que, según el caso, el hecho podría calificarse como estafa.

Además, desde 2025 la estafa se agrava cuando se manipula la voz o la imagen de otra persona con inteligencia artificial (Ley N.° 32314, 2025). La calificación final corresponde a la Fiscalía y al Poder Judicial en cada caso.

Entre 2020 y 2025, las denuncias por fraude informático crecieron casi 600%: pasaron de 4,259 a 29,342. Solo entre enero y setiembre de 2026 ya suman 26,305. De conservarse la tendencia, el 2026 puede cerrar con una cifra muy superior a la de 2025.

> **"El fraude informático creció casi 600% entre 2020 y 2025."**

Gráfico 6. Fraude informático: denuncias por año, 2020–2026



Nota: 2026 corresponde a enero–setiembre.
Fuente: Ministerio Público – Fiscalía de la Nación, registro de denuncias por delitos informáticos 2020–2026 (enero–setiembre).
Elaboración propia.

4.2. Suplantación de identidad: cuando alguien se hace pasar por ti

La suplantación de identidad (artículo 9 de la Ley N.° 30096) ocurre cuando una persona usa medios digitales para hacerse pasar por otra persona o por una empresa, y de ello resulta algún perjuicio material, moral o de otro tipo para la víctima. Para cometerla, el delincuente suele valerse de datos personales, fotografías o documentos de la persona suplantada, con el fin de obtener un beneficio indebido o de causarle daño. Es importante notar que la ley exige que exista un perjuicio.

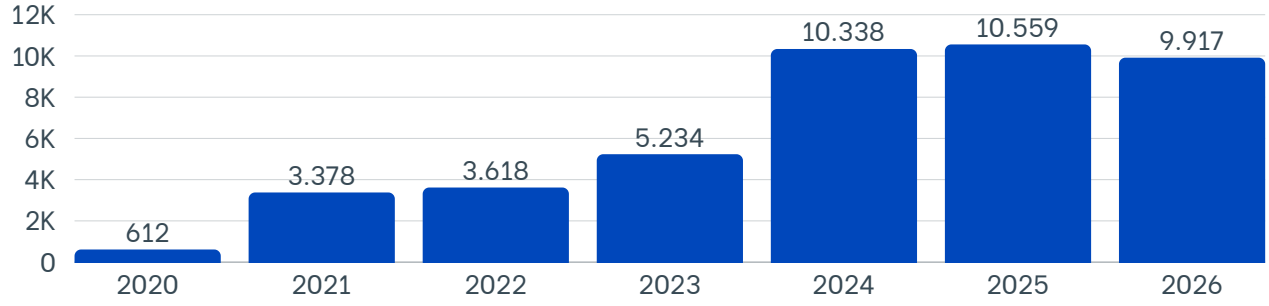
La pena es de 3 a 5 años de cárcel, y de 6 a 9 años cuando se suplanta la identidad de una persona menor de 18 años (Decreto Legislativo N.° 1591, 2023). Como en todos los delitos de esta ley, la pena puede aumentar si se usa inteligencia artificial o si actúa una organización criminal (Ley N.° 32314, 2025).

De acuerdo con el Ministerio Público (2024), los delincuentes informáticos realizan la suplantación de identidad para:

1. Cometer fraude financiero como compras en línea, transferencias bancarias, etc.
2. Obtener datos de otras personas de manera ilegal.
3. Cometer ciberbullying o acoso virtual.
4. Hacer grooming o ganar la confianza de un menor y cometer abuso sexual contra éste.

La suplantación de identidad es el delito informático de crecimiento más acelerado. Entre 2020 y 2025 sus denuncias se multiplicaron por 17: pasaron de 612 a 10,559 (+1,625%). El salto más fuerte ocurrió entre 2023 y 2024, cuando casi se duplicaron (de 5,234 a 10,338). Entre enero y setiembre de 2026 ya suman 9,917, el 94% del total de 2025.

Gráfico 7. Suplantación de identidad: denuncias por año, 2020–2026



Nota: 2026 corresponde a enero–setiembre.
Fuente: Ministerio Público – Fiscalía de la Nación, registro de denuncias por delitos informáticos 2020–2026 (enero–setiembre).
Elaboración propia.

5. ¿Dónde se denuncia más?

El Ministerio Público organiza su trabajo en distritos fiscales, que son las zonas del territorio en las que operan sus fiscalías. No siempre coinciden con los departamentos: Lima, por ejemplo, se divide en varios distritos fiscales.

Entre 2020 y setiembre de 2026, los distritos fiscales de Lima Centro, Lima Norte, Lima Este y Lima Sur concentraron 52.1% de todas las denuncias del país (104,252). Solo Lima Centro reúne casi una de cada cuatro (24.6%). Les siguen Lambayeque (5.4%), Arequipa (5.3%) y La Libertad (4.6%). En conjunto, los diez distritos fiscales con más denuncias suman 76.6% del total. El fraude informático es el delito más denunciado en todos los distritos fiscales, aunque su peso varía: representa 82% de las denuncias en Moquegua, pero menos de la mitad en Cañete (44%) y Apurímac (47%). La suplantación de identidad tiene un peso mayor al promedio nacional en Tacna (38%), Huánuco (34%) y Puno (33%).

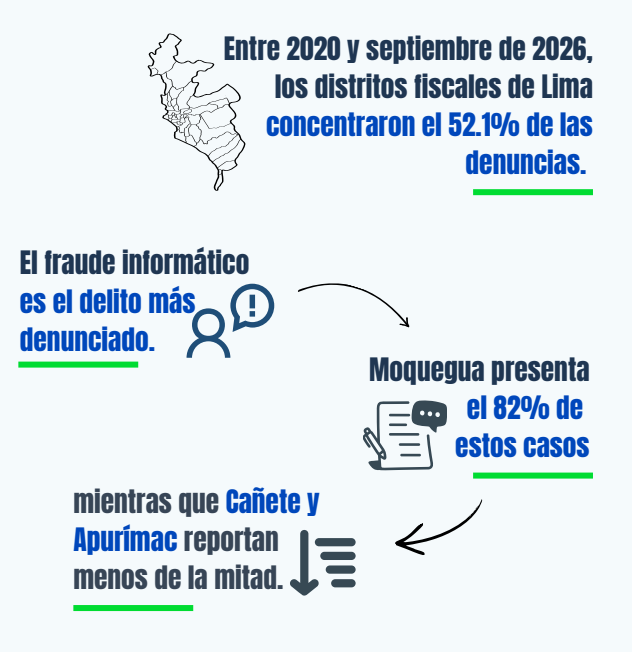


Tabla 2. Denuncias por delitos informáticos según distrito fiscal, 2020–2026

N°	Distrito Fiscal	Denuncias 2020–2026	% del total	Fraude informático (Art. 8)	Suplantación de identidad (Art. 9)
1	Lima Centro	49,257	24.6%	34,095	6,708
2	Lima Norte	20,85	10.4%	15,502	4,61
3	Lima Este	18,346	9.2%	13,141	4,616
4	Lima Sur	15,799	7.9%	12,171	3,234
5	Lambayeque	10,774	5.4%	6,488	2,679
6	Arequipa	10,671	5.3%	6,391	2,833
7	La Libertad	9,292	4.6%	5,233	2,466
8	Callao	7,089	3.5%	5,117	1,483

N°	Distrito Fiscal	Denuncias 2020–2026	% del total	Fraude informático (Art. 8)	Suplantación de identidad (Art. 9)
9	Piura	6,102	3.0%	4,004	1,902
10	Ica	5,09	2.5%	3,251	1,586
11	Cusco	4,186	2.1%	3,044	648
12	Huánuco	4,138	2.1%	2,122	1,417
13	Santa	3,334	1.7%	2,03	880
14	Junin	3,069	1.5%	2,053	625
15	Loreto	2,776	1.4%	2,13	402
16	Ayacucho	2,739	1.4%	1,567	649
17	Cajamarca	2,531	1.3%	1,642	737
18	Lima Noroeste	2,458	1.2%	1,647	489
19	Puno	2,174	1.1%	1,228	712
20	San Martin	2,129	1.1%	1,461	552
21	Moquegua	2,095	1.0%	1,717	274
22	Cañete	2,002	1.0%	876	422
23	Tacna	1,997	1.0%	1,101	752
24	Huaura	1,953	1.0%	1,424	440
25	Ucayali	1,608	0.8%	1,116	393
26	Sullana	1,396	0.7%	841	445
27	Amazonas	1,252	0.6%	726	375
28	Ancash	1,219	0.6%	673	372
29	Apurímac	895	0.4%	419	212

Nota: 2026 corresponde a enero–setiembre. El total incluye otros delitos informáticos, además del fraude y la suplantación.
Fuente: Ministerio Público – Fiscalía de la Nación, registro de denuncias por delitos informáticos 2020–2026 (enero–setiembre).
Elaboración propia.

N°	Distrito Fiscal	Denuncias 2020–2026	% del total	Fraude informático (Art. 8)	Suplantación de identidad (Art. 9)
30	Selva Central	827	0.4%	561	212
31	Madre De Dios	660	0.3%	440	154
32	Tumbes	560	0.3%	394	146
33	Pasco	555	0.3%	353	125
34	Huancavelica	367	0.2%	211	106
	Total	**200,190**	**100.0%**	**135,169**	**43,656**

Sin embargo, mirar solo el número de denuncias puede ser engañoso, porque los distritos fiscales con más población tienden a registrar más casos. Por eso es útil la tasa: el número de denuncias por cada 100 mil habitantes, que permite comparar territorios de distinto tamaño. Al comparar la tasa de denuncias por fraude informático entre 2021 y 2025, los distritos fiscales que más crecieron fueron Ayacucho, Sullana, Apurímac, Tumbes y Madre de Dios, donde la tasa se multiplicó entre 8 y 12 veces.

Tabla 3. Distritos fiscales con mayor crecimiento de la tasa de denuncias por fraude informático, 2021–2025 (por cada 100 mil habitantes)

Puesto	Distrito Fiscal	Tasa 2021	Tasa 2025	Var. %
1	Ayacucho	4.3	53.7	1,139.7%
2	Sullana	2.9	35.6	1,123.0%
3	Apurímac	2.3	28.0	1,106.0%
4	Tumbes	3.9	39.6	912.9%
5	Madre De Dios	7.8	66.0	746.9%

Fuente: Ministerio Público; población: INEI, Sistema de Información Regional para la Toma de Decisiones (SIRTOD).
Elaboración propia.

En el otro extremo, la tasa de Huaura prácticamente no varió (+9.7%), y Lima Noroeste, Piura, Callao y Santa tuvieron los menores aumentos. Un crecimiento bajo no significa necesariamente un problema menor: el Callao, por ejemplo, tiene la tasa más alta de este grupo (123.4 denuncias por cada 100 mil habitantes en 2025).

Tabla 4. Distritos fiscales con menor crecimiento de la tasa de denuncias por fraude informático, 2021–2025 (por cada 100 mil habitantes)

Puesto	Distrito Fiscal	Tasa 2021	Tasa 2025	Var. %
1	Huaura	30.0	33.0	9.7%
2	Lima Noroeste	22.6	38.4	69.9%
3	Piura	26.1	44.5	70.2%
4	Callao	66.7	123.4	85.1%
5	Santa	29.5	56.1	90.0%

Fuente: Ministerio Público; población: INEI, Sistema de Información Regional para la Toma de Decisiones (SIRTOD).
Elaboración propia.

¿Qué muestran las tasas entre 2021 y 2025?

- El delito se expande hacia regiones donde antes era menos frecuente. En 20 distritos fiscales, tanto el fraude como la suplantación de identidad crecieron más rápido que el promedio nacional. Los aumentos más fuertes se dan donde las tasas iniciales eran bajas: Ayacucho, Sullana y Apurímac superan +1,100% en fraude, y Loreto, Cañete y Tumbes superan +2,200% en suplantación de identidad.
- Lima Centro crece menos en porcentaje, pero más en volumen. En 4 distritos fiscales (Lima Centro, Ica, Lima Noroeste y Tacna) ambos delitos crecieron menos que el promedio nacional. En Lima Centro esto se explica porque ya partía de niveles muy altos: aun así, registró el mayor aumento absoluto en la tasa de fraude (+178 denuncias por cada 100 mil habitantes), seguido de Moquegua (+122).
- Huaura y Tacna, los casos de menor crecimiento. La tasa de fraude de Huaura casi no cambió (+9.7%). Tacna es el único distrito fiscal donde bajó la tasa de suplantación de identidad (–71.6%), aunque esto se explica en buena parte por un valor inusualmente alto en 2021 (79.7), que podría responder a un registro atípico.
- Ucayali no es comparable en suplantación de identidad, porque no registró denuncias por este delito en 2021.

6. Conclusiones



La ciberdelincuencia crece al ritmo de la vida digital.

La masificación de internet (que hoy llega a ocho de cada diez personas, casi siempre a través del celular) y el uso creciente de la banca electrónica han ampliado también las oportunidades para delinquir. Las denuncias por delitos informáticos se multiplicaron casi por cinco entre 2020 y 2025, y 2026 va camino de marcar un nuevo récord.



El problema se concentra en el bolsillo y la identidad de las personas.

El fraude informático y la suplantación de identidad explican casi nueve de cada diez denuncias por delitos informáticos, y su peso pasó de 56% en 2020 a 93% en 2025. Esto indica que la ciberdelincuencia que se denuncia en el país está orientada, sobre todo, a obtener dinero de personas comunes, por lo que la prevención debería priorizar estas dos amenazas.



La suplantación de identidad es el delito que más rápido crece.

Sus denuncias se multiplicaron por 17 entre 2020 y 2025. Con frecuencia se combina con el fraude —por ejemplo, cuando se roba una cuenta de WhatsApp para pedir dinero a los contactos de la víctima—, lo que muestra que proteger los datos personales y los códigos de verificación es una primera línea de defensa.

La ley se ha actualizado, pero el reto está en hacerla cumplir.

Entre 2023 y 2026 se aprobaron numerosas reformas: penas más altas, sanciones por el uso de inteligencia artificial, por el tráfico de datos y por la activación ilegal de chips. Sin embargo, endurecer las penas no basta si la investigación no alcanza a los responsables. Como referencia, la Fiscalía especializada en ciberdelincuencia de Lima Centro recibió más de 17 mil denuncias en dos años y obtuvo 78 sentencias en ese periodo (Decreto Legislativo N.° 1614, 2023, exposición de motivos). Fortalecer las capacidades de investigación, la cooperación con bancos y empresas de telecomunicaciones, y la cooperación internacional en el marco del Convenio de Budapest resulta clave.

Es un fenómeno nacional, no solo limeño.

Lima concentra el mayor volumen de denuncias, pero el crecimiento más acelerado se observa en distritos fiscales que partían de niveles bajos, como Ayacucho, Sullana, Apurímac, Tumbes, Madre de Dios, Loreto y Cañete. Esto plantea la necesidad de contar con fiscalías y unidades policiales especializadas, así como con campañas de prevención, también fuera de la capital.

Las cifras muestran solo una parte del problema.

Los datos corresponden a denuncias, no a la totalidad de delitos, y una parte de ellas (5.3%) no registra el delito específico. Mejorar la calidad de los registros y complementarlos con encuestas de victimización permitiría dimensionar mejor el fenómeno. Al mismo tiempo, a medida que se conectan nuevos grupos de la población, la educación digital (especialmente para quienes tienen menos experiencia en el uso de la tecnología) se vuelve una herramienta de prevención tan importante como la sanción penal.

7. ¿Cómo evitar ser víctima de un delito informático?

La mayoría de fraudes y suplantaciones no ocurren porque los delincuentes "hackeen" a los bancos, sino porque logran engañar a las personas para que entreguen sus claves o códigos. Por eso, la Superintendencia de Banca, Seguros y AFP (SBS) señala que la mejor herramienta de prevención es detenerse unos segundos antes de hacer clic en un enlace, compartir un código o atender una llamada que pide actuar con urgencia (El Peruano, 2026).

A continuación, se presentan recomendaciones sencillas de organismos oficiales y especialistas (El Peruano, 2023, 2026; SBS, s. f.; Infobae, 2026a, b, c).

Para prevenir el fraude informático

1 No compartas tus claves



Nunca compartas tus claves, token ni códigos de verificación. Ningún banco te los pedirá por llamada, mensaje de texto, correo o redes sociales.

2 Desconfía de mensajes urgentes



Si te dicen que tu cuenta fue bloqueada o que debes "actualizar tus datos", no entres al enlace. Comunícate con tu banco por sus canales oficiales.

3 No abras enlaces sospechosos



No abras enlaces que te pidan datos o claves, ni mensajes de remitentes desconocidos.

4 Activa las alertas de tu banco



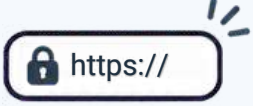
Activa las alertas de tu banco por mensaje de texto, correo o aplicación. Así sabrás al instante si alguien usa tu cuenta o tarjeta.

5 Evita el wifi público



No hagas operaciones bancarias ni compras con wifi público. Usa tu plan de datos o una red segura.

6 Compra solo en páginas seguras



Revisa que la dirección empiece con "https", que aparezca un candado y que sea la página oficial de la tienda.



Para prevenir la suplantación de identidad

1 Activa la verificación en dos pasos de WhatsApp



Así, aunque alguien obtenga tu código, necesitará además un PIN que solo tú conoces. Nunca compartas el código de seis dígitos que te envía WhatsApp.

2 Ponle una clave (PIN) al chip de tu celular



Así, si te roban el teléfono, nadie podrá usar tu chip en otro equipo. La clave que viene de fábrica suele ser fácil de adivinar, por lo que conviene cambiarla.

3 Revisa cuántas líneas de celular hay a tu nombre



Hazlo en la plataforma del Osiptel (checatuslineas.osiptel.gob.pe). Si encuentras una que no contrastase, puedes pedir que la den de baja.

4 Si pierdes la señal del celular, actúa de inmediato



Si pierdes la señal del celular sin motivo, comunícate de inmediato con tu operadora por otro medio. Puede ser un intento de duplicar tu chip.

5 Cuida tus datos personales



No los compartas por llamadas o mensajes.

6 Verifica antes de enviar dinero



Si un familiar o amigo te pide dinero con urgencia por mensaje, audio o videollamada, confirma por otro medio, por ejemplo, llamándolo a su número de siempre. Hoy la inteligencia artificial puede imitar voces y rostros.

¿Qué hacer si eres víctima de un delito informático?



Comunícate de inmediato con tu banco o billetera digital por sus canales oficiales, para bloquear cuentas, tarjetas u operaciones.



Guarda las pruebas: capturas de pantalla, mensajes, números de teléfono, enlaces y comprobantes.



Denuncia en cualquier comisaría, en la Dirección de Investigación de Ciberdelincuencia de la Policía Nacional o ante el Ministerio Público.



Nota metodológica

- Fuente de las denuncias: registro de denuncias por delitos informáticos del Ministerio Público – Fiscalía de la Nación [Base de datos: https://portal.mpfn.gob.pe/pedmp/index.php/dato/base-descarga]. El periodo analizado va de enero de 2020 a setiembre de 2026; para 2026 la información es parcial (enero–setiembre).

- Unidad de análisis: denuncias registradas. No equivalen a víctimas, a delitos comprobados ni a sentencias.

- Clasificación: las denuncias se agrupan según el artículo de la Ley N.° 30096 registrado. El 5.3% no cuenta con un delito específico registrado.

- Tasas: número de denuncias por cada 100 mil habitantes, calculado con estimaciones de población del Sistema de Información Regional para la Toma de Decisiones (SIRTOD). Las variaciones porcentuales y los promedios diarios fueron calculados por el equipo a partir de esta información.

- Uso de internet: los datos provienen de la Encuesta Nacional de Hogares (ENAHO) del INEI.

Referencias

- Congreso de la República. (2013, 22 de octubre). Ley N.° 30096, Ley de Delitos Informáticos. Diario Oficial El Peruano. https://leyes.congreso.gob.pe/Documentos/ExpVirPal/Texto_Consolidado/30096-TXM.pdf

- Congreso de la República. (2014, 10 de marzo). Ley N.° 30171, Ley que modifica la Ley 30096, Ley de Delitos Informáticos. Diario Oficial El Peruano.

- Congreso de la República. (2019, 13 de febrero). Resolución Legislativa N.° 30913, Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/1740637-2

- Congreso de la República. (2024, 11 de diciembre). Ley N.° 32183, Ley que modifica el Código Penal, Decreto Legislativo 635, para incorporar la modalidad de préstamos extorsivos en el tipo penal de extorsión. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/2352315-4

- Congreso de la República. (2025a, 29 de abril). Ley N.° 32314, Ley que modifica el Código Penal, Decreto Legislativo 635, y la Ley 30096, Ley de Delitos Informáticos, para incluir el uso de la inteligencia artificial en la comisión de delitos. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/2394851-2

- Congreso de la República. (2025b, 30 de setiembre). Ley N.° 32451, Ley que modifica la Ley 30096, Ley de Delitos Informáticos, y el Código Penal, Decreto Legislativo 635, respecto a la activación ilegal de líneas de servicios móviles y a la posesión ilegal de SIM card. Diario Oficial El Peruano.

- Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia (Serie de Tratados Europeos N.° 185). Budapest, 23 de noviembre de 2001.

- El Peruano. (2023, 22 de junio). ¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú. https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru

- El Peruano. (2025). Crecen denuncias de fraude informático, sobre todo de phishing y carding. https://elperuano.pe/noticia/277006-crecen-denuncias-de-fraude-informatico-sobre-todo-de-phishing-y-carding

- El Peruano. (2026, 14 de julio). ¿Recibiste dinero extra? Sigue estas recomendaciones para protegerlo de fraudes digitales. https://www.elperuano.pe/noticia/300246-recibiste-dinero-extra-sigue-estas-recomendaciones-para-protegerlo-de-fraudes-digitales

- Infobae. (2026a, 31 de mayo). Podrías tener líneas móviles a tu nombre y no saberlo: ¿cuáles son los peligros? https://www.infobae.com/peru/2026/05/31/podrias-tener-lineas-moviles-a-tu-nombre-y-no-saberlo-cues-son-los-peligros/

- Infobae. (2026b, 14 de agosto). Deepfakes y estafas románticas: así usan la IA los ciberdelincuentes para manipular a sus víctimas en Perú. https://www.infobae.com/peru/2026/08/14/deepfakes-y-estafas-romanticas-asi-usan-la-ia-los-ciberdelincuentes-para-manipular-a-sus-victimas-en-peru/

- Infobae. (2026c, 22 de octubre). Así es el nuevo método para robar cuentas de WhatsApp en Perú con un código aparentemente inofensivo. https://www.infobae.com/peru/2026/10/22/asi-es-el-nuevo-metodo-para-robar-cuentas-de-whatsapp-en-peru-con-un-codigo-aparentemente-inofensivo/

- Instituto Nacional de Estadística e Informática. (s. f.). Encuesta Nacional de Hogares (ENAHO), 2019–2025 [Base de datos]. INEI.

- Instituto Nacional de Estadística e Informática. (s. f.). Sistema de Información Regional para la Toma de Decisiones (SIRTOD) [Base de datos]. Recuperado en julio de 2026, de https://sirtod.inei.gob.pe/app/consulta

- Ministerio Público – Fiscalía de la Nación. (2024). Suplantación de identidad. https://www.gob.pe/25712-suplantacion-de-identidad

- Ministerio Público – Fiscalía de la Nación. (2026). Denuncias por delitos informáticos, 2020–2026 (enero–setiembre) [Base de datos].

- Poder Ejecutivo. (1991). Decreto Legislativo N.° 635, Código Penal. Diario Oficial El Peruano.

- Poder Ejecutivo. (2023a, 13 de diciembre). Decreto Legislativo N.° 1591, Decreto Legislativo que modifica la Ley N.° 30096, Ley de Delitos Informáticos, para promover el uso seguro y responsable de las tecnologías digitales por niñas, niños y adolescentes. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/2243815-1

- Poder Ejecutivo. (2023b, 21 de diciembre). Decreto Legislativo N.° 1614, Decreto Legislativo que modifica la Ley N.° 30096, Ley de Delitos Informáticos, para prevenir y hacer frente a la ciberdelincuencia [incluye exposición de motivos]. Diario Oficial El Peruano. https://www.congreso.gob.pe/Docs/comisiones2023/Constitucion/files/dl-1614-2023-of.pdf

- Poder Ejecutivo. (2024, 8 de agosto). Decreto Legislativo N.° 1625, Decreto Legislativo que modifica los artículos 154-B y 158 del Código Penal e incorpora el artículo 5-A en la Ley N.° 30096, Ley de Delitos Informáticos. Diario Oficial El Peruano.

- Poder Ejecutivo. (2026, 24 de enero). Decreto Legislativo N.° 1700, Decreto Legislativo que modifica la Ley N.° 30096, Ley de Delitos Informáticos, incorporando el delito de adquisición, posesión y tráfico ilícito de datos informáticos. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/2480387-2

- Superintendencia de Banca, Seguros y AFP. (s. f.). Fraudes digitales y telefónicos. https://www.sbs.gob.pe/usuarios/Fraudes-digitales-y-telefonicos

2026

GPS

La otra cara de la conexión:

la ciberdelincuencia en el Perú

2020 - 2026

@gpsagenciaperu