# ANÁLISIS DE LA CIBERDELINCUENCIA

**BOLETÍN**

EN ESTA EDICIÓN

## Ciberdelincuencia en el Ecuador: panorama nacional



**Dirección de Ciberdelitos**

**Ministerio del Interior**

Boletín de Análisis: Ciberdelincuencia en el Ecuador: panorama nacional

Ministerio del Interior

Subsecretaría de Combate al Delito

Dirección de Ciberdelitos

Presidente de la República

MAGISTER DANIEL NOBOA AZÍN

Ministro del Interior

Sr. JOHN REIMBERG OVIEDO

Subsecretario de Combate al Delito

TENIENTE CORONEL (SP) LUIS PÉREZ DÁVILA

Director de Ciberdelitos

TENIENTE CORONEL XAVIER GARZÓN PÉREZ

Responsables y Colaboradores

*Redacción del documento:*

INGENIERO CÉSAR TRELLES SEGOVIA, Analista de Ciberdelitos

INGENIERO FABIÁN SILVA TOLEDO, Analista de Ciberdelitos

MAGÍSTER GABRIEL REINOSO MARTÍNEZ, Analista de Ciberdelitos

*Redacción, edición y adaptación:*

MAGÍSTER DUVAL MONTATIXE CAIZALUISA, Analista de Ciberdelitos

MAGÍSTER CARLOS SIMBAÑA COBA, Analista de Ciberdelitos

*Redacción y revisión del documento:*

MAGÍSTER JORGE NÉJER GUERRERO, Especialista de Ciberdelitos

INGENIERO FREDDY GALLARDO SOSA, Especialista de Ciberdelitos

*JUNIO, 2026*

EL NUEVO ECUADOR Ministerio del Interior

# Contenido

# 1. SÍNTESIS DEL BOLETÍN

El presente boletín analiza la ciberdelincuencia en Ecuador: cómo se ejecuta, a quién afecta, qué muestran los datos oficiales y qué acciones sostiene el Estado frente a este fenómeno. El documento permite reconocer señales de alerta, reducir la exposición digital y activar canales institucionales de denuncia.

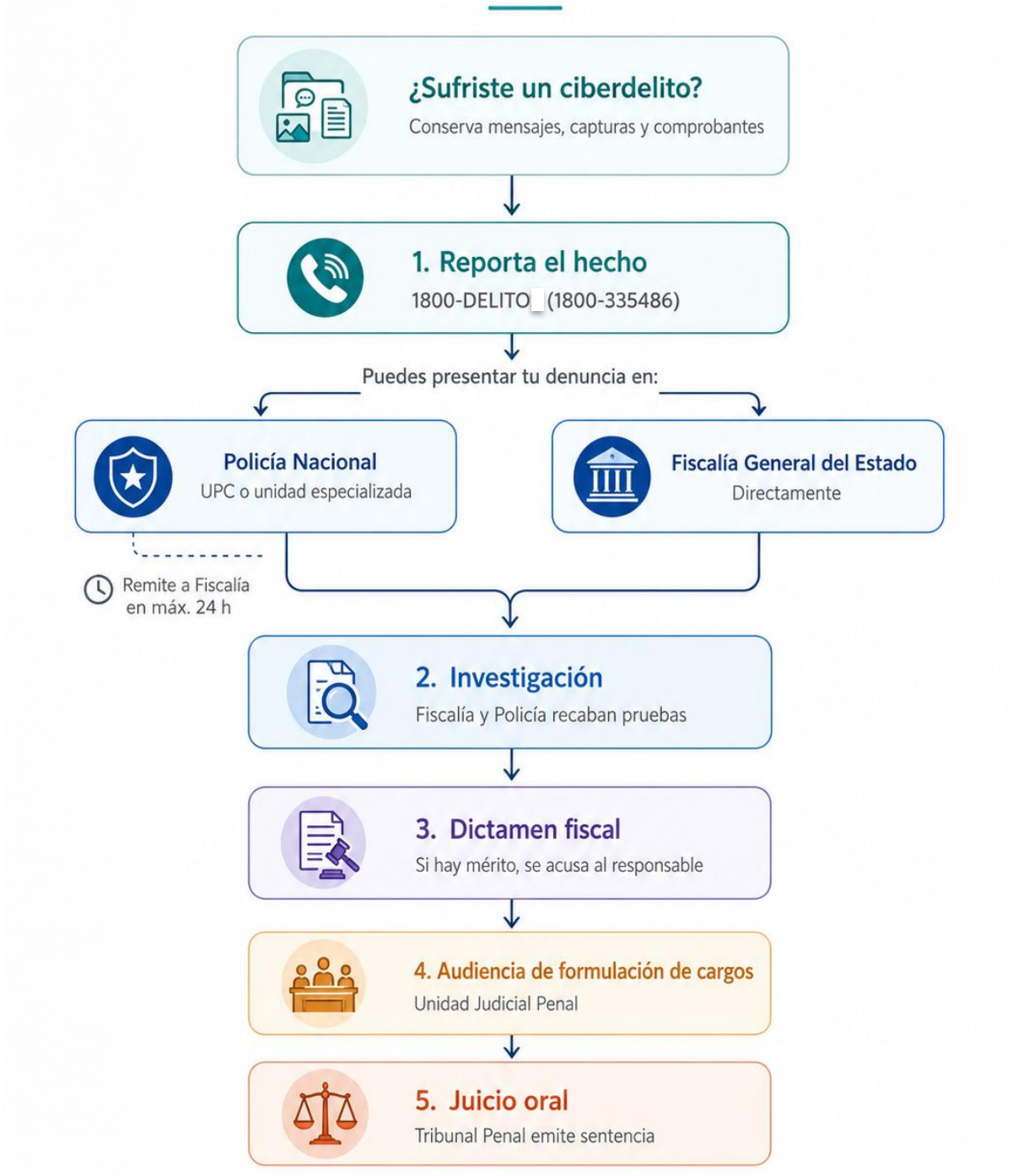
Entre 2022 y 2025, las noticias de delitos cometidos mediante tecnologías de la información y comunicación (TIC) aumentaron un 57,7%, con 11.606 registros en el último año según datos proporcionados por la Fiscalía General del Estado. Las modalidades de mayor incidencia son la apropiación fraudulenta por medios electrónicos, la violación a la intimidad y las estafas, perpetradas mediante engaño digital y uso inapropiado de inteligencia artificial.

El impacto y las consecuencias van más allá de la pérdida económica, ya que puede afectar la identidad digital, la salud emocional, la reputación personal e institucional; puede vulnerar la privacidad y disminuir la confianza en servicios esenciales. Los adultos mayores, niñas, niños y adolescentes, personas con discapacidad y ciudadanos con baja alfabetización digital son grupos especialmente vulnerables, ya que su exposición aumenta en actividades cotidianas como abrir un enlace, responder un mensaje, descargar un archivo, compartir una contraseña o aceptar contacto de un perfil desconocido.

## Acciones inmediatas dirigidas a la ciudadanía:

- Configurar sus cuentas con doble factor de autenticación, de tal forma que, al iniciar sesión, se solicite una verificación adicional, como un código enviado al teléfono celular, una notificación de aprobación o el uso de biometría.
- Confirmar la información directamente con la institución correspondiente, mediante sus canales oficiales, antes de entregar datos personales, abrir enlaces, descargar archivos o transferir dinero.
- Si en el entorno existen niñas, niños o adolescentes, la persona adulta debe escuchar sin juzgar, orientar a tiempo y mantener un canal de confianza. La escucha cercana reduce la búsqueda de apoyo en espacios digitales desconocidos.
- Ante un incidente digital, desconectar el dispositivo afectado de internet, guardar mensajes, capturas, comprobantes y otros elementos relevantes; reportar el hecho al 1800-DELITO (1800-335486) o ECU911 y presentar la denuncia ante la Fiscalía General del Estado.

***Gráfico 1:*** *Proceso para reportar o denunciar un ciberdelito*




***Elaboración:*** *Dirección de Ciberdelitos - Ministerio del Interior*

# 2. INTRODUCCIÓN

Según las noticias del delito registradas en la Fiscalía General del Estado, durante 2025 se receptó, en promedio, una noticia relacionada con presuntos delitos cometidos mediante el uso de tecnologías de la información y comunicación (TIC) cada 45 minutos. Este dato evidencia que la afectación digital alcanza espacios cotidianos, como banca digital, redes sociales, mensajería, comercio electrónico y trámites en línea. La conectividad avanza más rápido que la cultura preventiva, la alfabetización digital y las capacidades especializadas de protección, brecha que es aprovechada por estructuras delictivas para engañar, ocultar identidades, captar víctimas, incluidas niñas, niños y adolescentes (NNA), y causar perjuicios económicos, personales e institucionales.

Entre 2022 y 2025, las noticias del delito por conductas cometidas mediante tecnologías de la información y comunicación, registradas ante la Fiscalía General del Estado, aumentaron un 57,7%, al pasar de 7.465 en 2022 a 11.606 en 2025. Las modalidades de mayor incidencia - apropiación fraudulenta por medios electrónicos, violación a la intimidad y estafas- evidencian el uso de engaño digital, suplantación de identidad y el uso de inteligencia artificial con fines ilícitos. Estos hechos pueden traducirse en afectaciones, tales como pérdida patrimonial, exposición de datos, daño emocional, afectación reputacional y pérdida de confianza en servicios digitales.

Este Boletín de Análisis sobre la Ciberdelincuencia examina las formas de ejecución de las principales conductas delictivas en entornos digitales, analiza información oficial de la Fiscalía General del Estado, la Policía Nacional y el Consejo de la Judicatura, y contrasta el contexto nacional con tendencias regionales e internacionales documentadas por INTERPOL, Europol, el FBI y el BID. El documento incluye señales de alerta, medidas de prevención, actuación ante incidentes, acciones estatales y canales de denuncia.

El propósito del boletín es fortalecer la comprensión ciudadana con acciones concretas para detectar riesgos, verificar información, proteger datos, conservar evidencia y denunciar oportunamente. La información se sustenta en fuentes primarias verificadas y en el análisis técnico de la Dirección de Ciberdelitos del Ministerio del Interior del Ecuador.

# 3. OBJETIVO

Analizar la evolución de la ciberdelincuencia en el Ecuador, identificando sus principales causas, tendencias, modalidades y factores de riesgo, así como examinar las acciones del Estado en el ámbito normativo, institucional y de política pública orientadas a la protección ciudadana, con el propósito de generar insumos estratégicos que fortalezcan la prevención, detección y respuesta frente a los delitos cometidos mediante tecnologías de la información y comunicación (TIC).

# 4. DESARROLLO DEL TEMA

## Dinámica del delito

### Panorama y configuración del Delito

La ciberdelincuencia en Ecuador es una amenaza creciente, agravada por el uso de herramientas de inteligencia artificial. Se configura cuando internet y los dispositivos tecnológicos son el medio o el objeto de un delito, afectando a ciudadanos, empresas e instituciones públicas. Las conductas delictivas más reportadas ante la Fiscalía General del Estado son la apropiación fraudulenta por medios electrónicos, la violación a la intimidad y la estafa, tipificadas en el Código Orgánico Integral Penal (COIP). Frente a este escenario, el Estado prioriza la protección ciudadana y de las infraestructuras críticas mediante la articulación institucional a través del Ministerio del Interior, el Ministerio de Telecomunicaciones y Sociedad de la Información y el Ministerio de Defensa Nacional (1).

### Causas y Factores de Vulnerabilidad

La ciberdelincuencia aprovecha tres brechas fundamentales que se pueden identificar y reducir con prevención y control:

- **El factor humano:** Baja o limitada cultura digital, exceso de confianza y poca verificación antes de abrir enlaces, entregar datos, transferir dinero o sostener contacto con perfiles desconocidos, brecha que se amplía en niñas, niños y adolescentes cuando el acompañamiento familiar en el uso de dispositivos es limitado.
- **Vulnerabilidades tecnológicas**: El uso de contraseñas débiles o repetidas, la falta de actualizaciones de software en los dispositivos y la divulgación accidental de información.
- **Exposición de datos:** Las filtraciones masivas de información personal facilitan que los atacantes personalicen sus estafas para hacerlas más convincentes.

Entre otras causas que facilitan un ataque se destacan la vulnerabilidad de los sistemas, la pérdida o robo de dispositivos, personal con intenciones delictivas, brechas en controles y modalidades de ingeniería social (2).

## Manifestaciones más Frecuentes

- Los delincuentes utilizan engaño digital y manipulación psicológica para inducir a la víctima a entregar datos, dinero o acceso a cuentas. Las modalidades más frecuentes son:
- Mensajes falsos que aparentan provenir de bancos o instituciones públicas (ej. Agencia Nacional de Tránsito, Registro Civil) para robar credenciales.
- Amenazas de difusión de información íntima o privada con una finalidad clara de extorsión.
- Ofertas falsas, generalmente en redes sociales, respecto a productos, empleos, becas o beneficios que exigen pagos previos (3).
- Acercamientos sostenidos en redes sociales o aplicaciones de mensajería que construyen cercanía o confianza con niñas, niños y adolescentes, previos a solicitar información personal o contenido sensible.

## Dinámica de la ciberdelincuencia: formas de operación y afectación

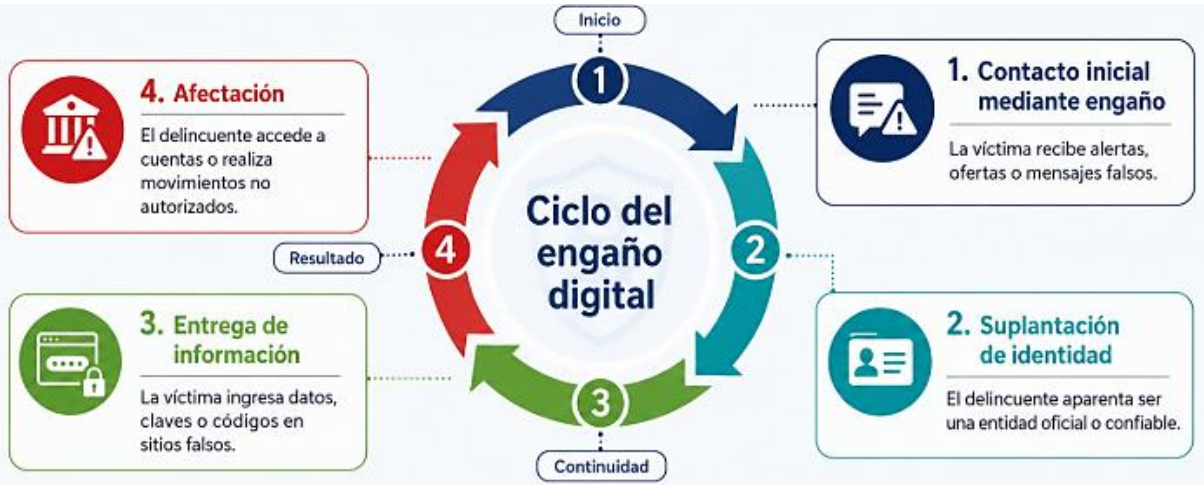
Las estructuras delictivas actúan de forma organizada: reclutan perfiles técnicos especializados, separan tareas, reutilizan engaños, compran o venden datos y buscan obtener dinero, acceso a cuentas o información sensible. El daño suele iniciar con un mensaje convincente y puede terminar en pérdida de dinero, exposición de información, extorsión o uso indebido de la identidad de la víctima para cometer otros ilícitos (5).

El ciclo habitual del engaño comprende de cuatro momentos:

1. Contacto inicial mediante engaño: La víctima recibe un mensaje urgente, una alerta falsa o una oferta demasiado conveniente. Ejemplo: "Su cuenta será bloqueada, ingrese aquí para validar sus datos" o "Gane un bono del gobierno".
2. La suplantación: El mensaje usa nombres, logos o direcciones parecidas a entidades reales para generar confianza y redirige a un sitio web falso idéntico al real para robar información.
3. La acción de la víctima: La persona ingresa sus datos personales, usuario y contraseña creyendo que interactúa con un canal seguro, lo que permite que los datos lleguen directamente al ciberdelincuente.

4. El impacto: El delincuente accede a cuentas bancarias, roba dinero o usa la identidad de la víctima para estafar a sus contactos.

***Gráfico 2:*** *Modus Operandi - La Trampa Digital: ¿Cómo actúan los ciberdelincuentes?*




***Elaboración:*** *Dirección de Ciberdelitos - Ministerio del Interior*

## Análisis del contexto nacional

El contexto nacional muestra que la ciberdelincuencia no opera separada de otros fenómenos delictivos. Economías ilícitas vinculadas a extorsión, tráfico ilícito de sustancias catalogadas sujetas a fiscalización, minería ilegal y lavado de activos pueden utilizar entornos digitales para contactar víctimas, mover recursos, ocultar identidades o coordinar actividades. Según el informe ESET 2025 sobre amenazas en América Latina, Ecuador registró 85.315 detecciones de programas usados para robar credenciales e información financiera, lo que evidencia exposición de datos y necesidad de fortalecer hábitos de seguridad digital (6).

### Marco normativo vigente

El país cuenta con instrumentos normativos que fortalecen la prevención, investigación y sanción de delitos cometidos mediante el uso de tecnologías de la información y comunicación:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Registro Oficial 557, 17/04/2002).
- Ley Orgánica de Telecomunicaciones (Tercer suplemento, Registro Oficial 439, 18/02/2015).
- Ley Orgánica de Protección de Datos Personales (Quinto suplemento, Registro Oficial 459, 26/05/2021).
- Ley Orgánica para la Transformación Digital y Audiovisual (Tercer suplemento, Registro Oficial 245, 07/02/2023).

- Adhesión al Convenio de Budapest sobre Ciberdelincuencia (12/12/2024).
- Manual de Actuación para la recolección, preservación y análisis de contenido digital (Registro Oficial Suplemento 113, 29/08/2025).
- Ley Orgánica para el Fortalecimiento de la Ciberseguridad (Quinto suplemento, Registro Oficial 290, 22/05/2026).
- Código Orgánico Integral Penal (Registro Oficial 180, reforma: Séptimo Suplemento, Registro Oficial 151, 24/10/2025).

# Estadísticas del fenómeno de la Ciberdelincuencia en Ecuador

## Fiscalía General del Estado

Las estadísticas proporcionadas por la Fiscalía General del Estado permiten identificar las noticias del delito asociadas a economías delictivas que incorporan el uso de herramientas digitales como medio para facilitar su planificación, ejecución o financiamiento. La Tabla 1 presenta una visión general de estas manifestaciones delictivas, constituyendo un insumo para comprender la convergencia entre la criminalidad tradicional y el entorno digital, así como para orientar acciones de prevención, investigación y formulación de políticas públicas.

***Tabla 1:*** *Noticias del delito - delitos relacionados con las economías delictivas, periodo 2022-2025*

| **Noticias del delito: Delitos relacionados con las economías delictivas** | **2022** | **2023** | **2024** | **2025** |
|---|---|---|---|---|
| Extorsión | 8.398 | 21.810 | 23.081 | 16.130 |
| Tráfico ilícito de sustancias catalogadas sujetas a fiscalización | 10.894 | 8.936 | 9.452 | 9.297 |
| Secuestro extorsivo | 574 | 1.450 | 1.900 | 1.627 |
| Tráfico ilícito de armas de fuego, armas químicas, nucleares o biológicas | 232 | 334 | 741 | 622 |
| Tráfico ilícito de migrantes | 121 | 142 | 114 | 47 |
| Extorsión sexual | 80 | 156 | 164 | 187 |
| Trata de personas | 99 | 113 | 95 | 125 |
| Lavado de activos | 48 | 58 | 73 | 81 |
| Total | **20.446** | **32.999** | **35.620** | **28.116** |

***Elaboración:*** *Dirección de Ciberdelitos - Ministerio del Interior.*
***Fuente****: Fiscalía General del Estado*

Por otra parte, la Tabla 2 presenta las noticias del delito registradas por la Fiscalía General del Estado relacionadas con presuntos delitos cometidos mediante el uso de las tecnologías de la información y la comunicación (TIC). Esta información permite analizar la evolución de la ciberdelincuencia, identificar tendencias y patrones del fenómeno delictivo digital, así como generar evidencia que contribuya al diseño de estrategias de prevención y a la formulación de política pública orientadas a combatir este fenómeno.

***Tabla 2:*** *Noticias del Delito - Delitos cometidos mediante el uso de TIC, periodo 2022-2025.*

| **Delitos cometidos mediante el uso de TIC periodo 2022 -2025** | | | | |
|---|---|---|---|---|
| **Año 2022** | **Año 2023** | **Año 2024** | **Año 2025** | **Total** |
| 7.465 | 8.313 | 9.497 | 11.606 | **36.881** |

***Elaboración:*** *Dirección de ciberdelitos.*
***Fuente****: Fiscalía General del Estado*

Según los registros de la Fiscalía General del Estado, las denuncias de delitos cometidos mediante tecnologías de la información y comunicación (TIC) pasaron de 7.465 registros en 2022 a 11.606 en 2025, lo que representa un crecimiento acumulado aproximado del 57,7%. Entre 2024 y 2025, el incremento fue del 24,3%. Las modalidades de mayor incidencia son la apropiación fraudulenta por medios electrónicos, la violación a la intimidad y las estafas.

## Unidad Nacional de Ciberdelito de la Policía Nacional

La información proporcionada por la Unidad Nacional de Ciberdelito de la Policía Nacional corresponde a delegaciones oficiales emitidas por autoridad competente en investigaciones sobre delitos cometidos mediante tecnologías de la información y comunicación (TIC), durante el período 2022- 2025. La Tabla 3 muestra la demanda investigativa especializada en materia de ciberdelincuencia y permite analizar la evolución de las investigaciones, identificar tendencias en la actividad operativa y fortalecer la toma de decisiones para la planificación de estrategias de prevención, investigación y persecución penal.

***Tabla 3:*** *Delegaciones por delitos con el uso de las TIC periodo 2022-2025*

| **Delegaciones de Delitos cometidos con el uso de las TIC periodo 2022-2025** | | | | |
|---|---|---|---|---|
| **Año 2022** | **Año 2023** | **Año 2024** | **Año 2025** | **Total** |
| 1.039 | 858 | 880 | 968 | **3.745** |

***Elaboración:*** *Dirección de Ciberdelitos.*
***Fuente:*** *Unidad Nacional de Ciberdelito de la Policía*

Entre 2022 y 2025 se registraron 3.745 delegaciones, lo que evidencia una actividad investigativa sostenida frente a conductas delictivas cometidas mediante TIC. Las tipologías

más representativas son la apropiación fraudulenta por medios electrónicos, el acceso no consentido a un sistema informático, telemático o de telecomunicaciones, la violación a la intimidad y la estafa.

## Consejo de la Judicatura

Entre 2022 y 2025, el Consejo de la Judicatura registró 1.772 causas ingresadas y 1.387 causas resueltas por delitos cometidos mediante el uso de tecnologías de la información y comunicación (TIC), con un índice general de resolución del 78,3%.

La Tabla 4 presenta la información proporcionada por el Consejo de la Judicatura sobre las causas ingresadas y resueltas por delitos cometidos mediante el uso de tecnologías de la información y la comunicación (TIC) durante el período 2022–2025. La mayor cantidad de causas ingresadas se concentró en 2023, con 485 casos; en 2025 el ingreso descendió a 372. Las causas resueltas pasaron de 411 en 2022 a 209 en 2025. Esta variación puede responder a mayor complejidad probatoria, necesidad de análisis técnico y tiempos procesales propios de delitos con evidencia digital.

***Tabla 4:*** *Causas ingresadas y causas resueltas de delitos con el uso de las TIC periodo 2022-2025*

| **Causas ingresada y resueltas periodos 2022 - 2025** | | | | | |
|---|---|---|---|---|---|
| | **Año 2022** | **Año 2023** | **Año 2024** | **Año 2025** | **Total** |
| Causas ingresadas | 471 | 485 | 444 | 372 | **1.772** |
| Causas resueltas | 411 | 414 | 353 | 209 | **1.387** |

***Elaboración:*** *Dirección de ciberdelitos.*
***Fuente:*** *Consejo de la judicatura*

# Tendencias internacionales de la ciberdelincuencia

La ciberdelincuencia constituye un riesgo delictivo transnacional. Los actores explotan la conectividad, el uso masivo de plataformas tecnológicas, la exposición de datos personales y las brechas de cultura preventiva. Esta realidad trasciende fronteras y exige respuestas coordinadas, preventivas e investigativas. Además, informes recientes advierten un cambio en la lógica del atacante, con menos ruido técnico, mayor persistencia y mayor impacto económico, operativo y reputacional (15).

El “Internet Crime Complaint Center” del FBI registró en 2024 un total de 859.532 denuncias y pérdidas reportadas superiores a USD 16.600 millones, lo que representó un incremento aproximado del 33% frente a 2023 (7). Estas cifras, propias del contexto norteamericano,

ilustran la escala económica que alcanzan los fraudes en línea, la suplantación de identidad y el compromiso de cuentas.

En cuanto a operaciones internacionales, la Operación Serengeti de INTERPOL (2024), ejecutada en 19 países africanos, derivó en 1.006 detenidos, el desmantelamiento de 134.089 infraestructuras maliciosas, la identificación de más de 35.000 víctimas y pérdidas vinculadas cercanas a USD 193 millones (8). Estos datos muestran que las estructuras dedicadas a la ciberdelincuencia operan de forma distribuida, emplean infraestructura tecnológica transfronteriza y afectan simultáneamente a miles de personas en distintos territorios.

La Operación HAECHI VI de INTERPOL (abril–agosto 2025), en 40 países, recuperó USD 439 millones; USD 342 millones en monedas digitales y USD 97 millones en activos físicos y virtuales, enfocándose en phishing de voz, fraudes sentimentales, extorsión sexual, fraudes de inversión, cuentas de correo empresarial comprometidas y lavado de activos en línea (9).

En América Latina y el Caribe, el Reporte de Ciberseguridad 2025, elaborado por el Banco Interamericano de Desarrollo, la Organización de los Estados Americanos y el Global Cyber Security Capacity Centre de la Universidad de Oxford, evaluó la madurez de ciberseguridad de 30 países. El informe registra avances regionales desde 2020 en las cinco dimensiones analizadas; sin embargo, identifica desafíos persistentes en recursos, talento especializado, coordinación intersectorial, protección de infraestructura crítica, investigación, innovación y consolidación de mercados de ciberseguridad (10).

Europol advierte que los datos personales, las credenciales de acceso y las identidades digitales se han convertido en activos de alto valor para una economía clandestina basada en el robo, intercambio y explotación de información, cuyo alcance se agrava con el uso indebido de inteligencia artificial. Estas herramientas permiten generar mensajes convincentes, contenidos multilingües e imitaciones realistas de voz o imagen, facilitando fraudes, extorsión, ransomware, compromiso de cuentas y otras conductas ilícitas que afectan a ciudadanos, funcionarios y organizaciones (11).

Las amenazas masivas confirman la persistencia del phishing y los engaños en línea como modalidades de alta incidencia. Kaspersky reportó que en 2024 sus sistemas bloquearon más de 893 millones de intentos de phishing a escala global, un incremento aproximado del 26% frente a 2023 (12). Esta cifra evidencia esquemas basados en manipulación, suplantación y engaño, especialmente durante períodos de alta actividad comercial, uso intensivo de servicios financieros, compras en línea, turismo, campañas promocionales y trámites en línea.

Para Ecuador, el panorama regional e internacional es relevante porque las modalidades observadas en otros países muestran cómo la ciberdelincuencia se adapta a los hábitos digitales de la población y puede trasladarse al entorno nacional mediante redes sociales, mensajería instantánea, comercio electrónico, servicios financieros, activos virtuales, correos electrónicos y páginas web fraudulentas. Esta observación permite identificar indicios relevantes para la acción pública: fortalecer la prevención ciudadana, promover la denuncia oportuna, proteger los datos personales, preservar evidencia electrónica, sostener la cooperación internacional y mantener capacidades institucionales orientadas a prevenir, detectar e investigar delitos cometidos mediante tecnologías de la información y comunicación (TIC).

## Efectos de la ciberdelincuencia

Uno de los efectos más graves de la ciberdelincuencia es el daño psicológico, especialmente en casos de extorsión con contenido íntimo, acoso en línea o publicación de datos personales sin consentimiento, suplantación de identidad o difusión de contenidos íntimos (16). Las víctimas suelen experimentar ansiedad, depresión, trastornos del sueño, sensación de persecución o miedo a utilizar medios digitales. El sentimiento de vulnerabilidad que provoca la intromisión no consentida en la intimidad, unido a la incertidumbre sobre el uso futuro de los datos expuestos, genera una angustia persistente que puede prolongarse mucho después de haber sufrido el incidente (18).

En el plano social, la ciberdelincuencia puede afectar gravemente la reputación de las personas. La difusión de contenidos íntimos, la manipulación de perfiles en redes sociales, la publicación de datos privados o la suplantación de identidad pueden tener consecuencias irreversibles, tanto en el ámbito personal como profesional. En casos extremos, como el acoso sistemático en redes sociales o la exposición pública de imágenes íntimas, el impacto emocional puede derivar en aislamiento social, abandono académico o laboral, o incluso pensamientos suicidas, especialmente en adolescentes y jóvenes (18).

En el ámbito económico, los efectos de la ciberdelincuencia también son relevantes. Muchas víctimas sufren pérdidas directas a través de fraudes bancarios, suplantación de identidad o compras no autorizadas, enfrentándose luego a largos y confusos procedimientos legales para recuperar sus fondos o limpiar su historial crediticio. En los casos de ransomware, las empresas y particulares pueden afrontar pagos de rescate para recuperar el acceso a sus datos, y no siempre con garantías de éxito. Las consecuencias financieras pueden extenderse incluso a las

víctimas indirectas, como los clientes de empresas afectadas por filtraciones de datos o los ciudadanos cuyas instituciones públicas han sido atacadas (14).

Otro efecto importante es la pérdida de confianza en la tecnología. Muchas víctimas, tras sufrir un ataque, desarrollan desconfianza hacia plataformas digitales, redes sociales o servicios online. Esto puede traducirse en una reducción del uso de herramientas tecnológicas, en un mayor aislamiento digital o en una renuncia al aprovechamiento de las ventajas que ofrece la sociedad de la información. Esta desconfianza afecta también a la percepción de seguridad institucional, especialmente cuando las víctimas sienten que no han recibido una respuesta adecuada por parte de las autoridades o que su denuncia ha sido ignorada, archivada o nunca resuelta.

Conviene señalar que el impacto de la ciberdelincuencia se amplifica en contextos de desigualdad, falta de recursos o baja alfabetización digital. Las personas adultas mayores, niñas, niños y adolescentes y personas con discapacidad son susceptibles de ser víctimas, ya que suelen tener menos herramientas para identificar amenazas, proteger su información o responder eficazmente ante una situación de riesgo. Esta desigualdad digital se convierte así en un factor de victimización secundaria que perpetúa los efectos del delito y agrava las consecuencias sociales.

El sector empresarial registra una afectación relevante por los ciberataques, junto con gobiernos y organizaciones sin fines de lucro. En promedio, una organización tarda unos 280 días en detectar y contener un incidente de seguridad, lo que puede tener consecuencias económicas y reputacionales graves (20).

Desde un punto de vista legal y procedimental, las víctimas del delito cometido por medio de las TIC suelen enfrentarse a un sistema lento, fragmentado y poco preparado para dar respuesta a sus necesidades específicas. La dificultad para identificar a los agresores, especialmente cuando operan desde el extranjero o emplean técnicas de anonimato sofisticadas, limita en muchos casos las posibilidades de obtener justicia (21).

A continuación, se resume gráficamente el impacto que tienen los principales tipos de ciberdelitos sobre las víctimas, diferenciando sus consecuencias económicas, psicológicas y sociales (16).

***Tabla 5:*** *Impacto de la ciberdelincuencia en las víctimas*

| Tipo/Técnica de Ciberdelito | Impacto Económico | Impacto Psicológico | Impacto Social |
|---|---|---|---|
| Fraude Financiero | Pérdida de dinero por transacciones fraudulentas | Estrés y ansiedad por pérdida financiera | Pérdida de confianza en sistemas digitales |
| Suplantación de Identidad | Uso indebido de tarjetas y cuentas bancarias | Sensación de inseguridad y vulnerabilidad | Dificultad para realizar trámites y compras en línea |
| Ransomware | Pago de rescate por liberación de archivos | Desesperación ante la pérdida de datos | Desconfianza en la seguridad digital de las empresas |
| Ciberacoso y sextorsión | Gastos de asesoramiento legal y psicológico | Depresión y miedo por exposición pública | Aislamiento social y afectación de relaciones personales |
| Ciberataques a infraestructuras | Costos por restauración de sistemas dañados | Angustia por posible colapso de servicios esenciales | Crisis en sectores estratégicos como salud y finanzas |

***Elaboración:*** *Dirección de Ciberdelitos – MDI.*
***Fuente:*** *Universidad Europea (19)*

## Señales de alerta y actuación segura

En el entorno digital ecuatoriano, la detección temprana reduce la exposición de ciudadanos, instituciones y organizaciones frente a delitos cometidos mediante tecnologías de la información y comunicación (TIC). Las señales pueden presentarse como mensajes urgentes, solicitudes inusuales, perfiles falsos, enlaces alterados, archivos sospechosos o fallas técnicas en dispositivos y sistemas. Identificarlas a tiempo evita que el engaño avance hacia robo de dinero, suplantación de identidad, extorsión o secuestro de datos (22).

A continuación, se desglosan las principales señales de alerta clasificadas por sus modalidades más frecuentes en el entorno ecuatoriano:

***Tabla 6:*** *Señales de alerta en entornos digitales*

| Situación de riesgo | Posible intención delictiva | Acciones recomendadas |
|---|---|---|
| Mensajes con frases como “bloqueo de cuenta”, “verifique ahora”, “citación urgente”, “orden de captura”, “pagos inmediatos” o supuestos problemas legales. | Intento de presión para obtener datos, dinero o acceso a cuentas.<br>Ejemplo: “Citación legal de la Fiscalía General del Estado” identificada por CSIRT-EPN (23). | Detener la interacción, evitando enlaces o archivos, y verificar la información por medios institucionales. |
| Solicitud de contraseñas, códigos de seguridad o datos bancarios. | Engaño para tomar control de cuentas personales, financieras o institucionales. | Cerrar el mensaje o llamada y comunicarse directamente con la entidad.<br>Los canales oficiales gestionan información por vías verificables (24). |
| Enlaces o direcciones web que imitan canales oficiales, con errores mínimos, dominios extraños o nombres parecidos al original. | Página falsa diseñada para capturar datos. | Revisar la dirección web, remitente y dominio antes de ingresar información. |
| Perfiles desconocidos que generan confianza rápida, piden información sensible o trasladan la conversación a canales privados. | Captación digital para manipular, extorsionar o exponer a la víctima. | Cortar el contacto, guardar evidencia y denunciar si existen amenazas, exigencias de pago o presión para enviar material íntimo (25)(33).<br>En niñas, niños y adolescentes, contar con un cuidador de confianza del menor, facilita identificar la situación a tiempo. |
| Dispositivo lento, sobrecalentado, batería agotada sin causa aparente, antivirus desactivado, archivos modificados o mensajes de rescate. | Posible programa dañino, extracción de datos o secuestro de información. | Desconectar el equipo de internet y evitar manipular archivos hasta recibir orientación técnica (26). |
| Correos atribuidos a instituciones públicas enviados desde cuentas gratuitas, dominios extraños o con archivos inesperados. | Suplantación institucional para instalar programas dañinos o robar información. | Verificar el remitente oficial antes de abrir archivos o entregar datos (23). |

| | | |
|---|---|---|
| Cambios de cuenta bancaria de proveedores, transferencias fraccionadas o movimientos fuera del patrón habitual. | Posible fraude financiero en entornos comerciales o institucionales. | Confirmar fuera de línea con el proveedor o entidad antes de transferir fondos (27). |
| Notificaciones de premios, sorteos, bonos, beneficios o recompensas en los que la persona no ha participado. | Engaño para obtener datos personales, inducir pagos previos o dirigir a sitios falsos. | No entregar información ni realizar pagos.<br>Verificar la promoción en el canal oficial de la entidad mencionada. |

***Elaboración:*** *Dirección de Ciberdelitos – Ministerio del Interior*

La presión para enviar contenido íntimo, seguida de amenazas de difusión o exigencias de pago, debe tratarse como una señal inmediata de extorsión digital.

Reconocer estas señales convierte la prevención en una práctica diaria. Ante solicitudes urgentes, premios inesperados, enlaces dudosos, archivos no solicitados o cambios financieros sin verificación, la acción correcta es detenerse, comprobar la información por canales oficiales y conservar evidencia antes de interactuar, hacer clic o transferir fondos.

## Medidas de prevención y resiliencia digital

La seguridad absoluta en el ciberespacio no existe; por ello, la protección digital se basa en una regla práctica: detectar señales de alerta, verificar la información por canales oficiales, contener el daño, preservar evidencia y denunciar. Esta ruta debe complementarse con hábitos simples y sostenidos: leer antes de hacer clic, revisar remitentes y enlaces, configurar la seguridad de las cuentas, usar contraseñas diferentes, evitar compartirlas y activar una verificación adicional al inicio de sesión (10).

La prevención individual constituye la primera barrera defensiva contra los delitos informáticos. Diversas investigaciones en el entorno educativo y social ecuatoriano revelan que los atacantes explotan con frecuencia la confianza o el desconocimiento del usuario para obtener credenciales bancarias o datos reservados de forma voluntaria (10) (29). Los desafíos de articulación institucional y educación digital refuerzan la necesidad de medidas claras, sostenidas y fáciles de aplicar por usuarios, entidades públicas y organizaciones privadas (30) (31).

Ante este contexto, las medidas de protección personales propuestas se detallan a continuación:

***Tabla 7:*** *Medidas básicas de protección digital*

| Medida | Aplicación ciudadana | Utilidad |
|---|---|---|
| Doble verificación en cuentas. | Activarla en correo, redes sociales y banca digital. | Añade una barrera de protección, aunque la contraseña haya sido expuesta (34). |
| Actualizaciones permanentes. | Mantener sistema, aplicaciones, antivirus y dispositivos actualizados. | Corrige fallas conocidas que pueden ser usadas para robar información o instalar programas dañinos (35). |
| Verificación directa. | Ante pedidos de datos, pagos u ofertas exageradas, cerrar la interacción y contactar a la entidad por canales oficiales. | Evita decisiones tomadas bajo presión o engaño (36). |
| Cuidado en redes públicas. | Evitar transacciones sensibles en redes Wi-Fi abiertas. | Reduce la exposición de datos durante conexiones inseguras (37). |
| Autoaprendizaje continuo en seguridad digital | Investigar sobre diferentes métodos o señales de engaño, mensajes falsos y suplantación. | Disminuye clics en enlaces dañinos y entrega voluntaria de información (37). |
| Acompañamiento digital de niñas, niños y adolescentes. | El adulto responsable, cuidador, docente o referente cercano debe mantener una relación de confianza con la niña, niño o adolescente, para que tenga a quien acudir cuando algo le genere duda, presión, miedo o incomodidad. | Permite detectar a tiempo contactos de riesgo, pedidos indebidos de información, presión emocional o amenazas, y facilita al menor pedir ayuda sin temor. |

***Elaboración:*** *Dirección de Ciberdelitos – MDI.*

***Fuente:*** *Asociación de Bancos Privados del Ecuador (Asobanca) (37)*

## Actuación ante un presunto delito en el entorno digital

Si cree que ha sido víctima de un delito en internet o a través de medios digitales, actúe de inmediato. Los primeros minutos son importantes para reducir los daños, proteger su información y facilitar la investigación. La actuación ciudadana frente a un presunto delito en el entorno digital puede resumirse en tres acciones fundamentales: contener el incidente, preservar la evidencia y denunciar ante las autoridades competentes.

***Tabla 8:*** *Qué hacer ante un incidente digital*

| Paso | Acción prioritaria | Acción operativa |
|---|---|---|
| 1. Contener | Reducir el daño inicial. | Desconectar de internet el dispositivo afectado; ante fraude bancario, contactar a la entidad financiera correspondiente según sea el caso, bloquear cuentas o tarjetas; cambiar contraseñas desde un equipo seguro y cerrar sesiones abiertas (37). |
| 2. Preservar evidencia | Conservar elementos útiles para la investigación. | Guardar mensajes, capturas de pantalla, registros de transacciones, encabezados de correos, números de cuenta, enlaces, usuarios y cualquier dato relacionado. La evidencia digital debe mantenerse íntegra (38). |
| 3. Denunciar | Activar canales oficiales. | Reportar el hecho al 1800-DELITO (1800-335486) o ECU911 y presentar la denuncia ante la Fiscalía General del Estado. |

***Elaboración:*** *Dirección de Ciberdelitos*

Un delito en el entorno digital puede ocasionar pérdidas económicas, robo de identidad, acceso no autorizado a cuentas, exposición de información personal, afectaciones emocionales, daños a la reputación e interrupción de actividades, con consecuencias que pueden extenderse tanto al ámbito personal como al familiar y laboral.

En el caso de afectaciones financieras, la víctima debe presentar el reclamo ante su entidad financiera. Si el caso requiere escalamiento, puede acudir al Defensor del Cliente o utilizar el portal de reclamos de la Superintendencia de Bancos: https://www.superbancos.gob.ec/bancos/reclamos/ o en el caso de cooperativas de ahorro y crédito a la Superintendencia de Economía Popular y Solidaria (SEPS): https://recepciondocumental.seps.gob.ec/

***Gráfico 3:*** *Actuación ante un Ciberdelito*


***Elaboración:*** *Dirección de ciberdelitos - MDI*

## Acciones del Estado frente al delito.

Las acciones del Estado ecuatoriano frente a la ciberdelincuencia avanzan hacia una arquitectura institucional con roles definidos, instrumentos legales y capacidades técnicas en fortalecimiento. El punto estratégico es pasar de atender hechos aislados a analizar conductas repetitivas y sus interconexiones, muchas veces ocultas, para identificar elementos vinculados a estructuras delictivas.

La base normativa consolidada en los últimos años ha fortalecido las capacidades jurídicas e institucionales del Ecuador frente a la ciberdelincuencia. La Política Nacional de Ciberseguridad (5to. suplemento R.O. 479, 2021) y la Estrategia Nacional de Ciberseguridad (2022) establecieron una hoja de ruta con prioridades concretas: gobernanza digital, protección de infraestructuras críticas, cooperación internacional y formación de capacidades. La Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026) incorpora además obligaciones específicas para operadores de infraestructura crítica y mecanismos de reporte de incidentes, cerrando una brecha regulatoria que limitaba la capacidad de respuesta ante eventos de alto impacto.

La adhesión al Convenio de Budapest fortalece la capacidad estatal para actuar cuando la evidencia se encuentra fuera del país. Su valor operativo está en permitir solicitudes de preservación de datos, contacto con autoridades extranjeras mediante la Red 24/7 y uso de estándares comunes para evidencia digital. En delitos donde un mensaje, una cuenta o un registro puede desaparecer en minutos, la cooperación internacional se convierte en una condición determinante para la investigación.

En el plano operativo, la acción estatal se sostiene en funciones complementarias. La Dirección de Ciberdelitos del Ministerio del Interior aporta análisis estratégico, prevención, articulación interinstitucional e insumos para política pública, incluyendo el presente boletín y la organización del “II Congreso Internacional de Combate a la Ciberdelincuencia” (2026), que contó con la asistencia de diversos actores del Sector Público y Privado. La Unidad Nacional de Ciberdelito de la Policía Nacional desarrolla investigación especializada sobre hechos cometidos mediante tecnologías de la información y comunicación. La Unidad Nacional Especializada en Investigación de Ciberdelito de la Fiscalía General del Estado dirige la investigación penal, resguarda la validez de la evidencia digital y coordina con operadores de justicia (33). El valor radica en la conexión entre estas funciones para prevenir con información, investigar con evidencia y sostener la validez procesal de los casos.

Pasar de investigar incidentes individuales a desarticular las estructuras que los sostienen, en la práctica, implica correlacionar patrones entre denuncias aparentemente aisladas, rastrear el flujo de fondos a través de cuentas de tránsito y billeteras de criptoactivos, identificar infraestructuras compartidas entre distintos grupos como dominios, direcciones IP, servidores de comando y vincular perfiles digitales que operan bajo anonimato, entre otros. Ecuador trabaja en el fortalecimiento de capacidades para la integración de información proveniente de denuncias ciudadanas, reportes de entidades financieras, alertas de proveedores de servicios digitales y organismos internacionales, bajo principios de legalidad, protección de datos y proporcionalidad. La participación en la Red de Ciberinteligencia de INTERPOL y el acceso a herramientas de trazabilidad de activos virtuales, referenciadas en el marco de la UNODC, amplían la capacidad de seguir el rastro económico del delito. En el entorno digital, seguir el dinero suele ser tan importante como identificar al autor, pues permite comprender y desarticular las estructuras que sostienen la actividad delictiva.

La oportunidad de la respuesta estatal frente a la víctima es un factor clave de efectividad. La comunicación preventiva, las alertas tempranas, los canales accesibles y la protección de grupos con mayor exposición inciden directamente en que una persona realice la denuncia dentro del plazo establecido y mantenga evidencia útil para su caso.

Ecuador también participa en espacios de cooperación multilateral, donde el intercambio de información asociada a incidentes digitales apoya la investigación de casos y fortalece la prevención de amenazas.

El factor que determina si el marco legal y operativo construido se traduce en resultados concretos es el talento especializado. Un experto forense digital puede sostener una cadena de custodia válida ante el juez; un fiscal con conocimiento técnico puede convertir la evidencia digital en una acusación sólida; y un juez con formación específica puede resolver el caso con mayor comprensión de la prueba digital. La formación continua y especializada de policías, fiscales, jueces, peritos, analistas y funcionarios es clave para fortalecer la investigación, la judicialización y la respuesta institucional frente a la ciberdelincuencia.

# 5. CONCLUSIONES

- Entre 2022 y 2025, los registros de denuncias relacionadas con las TIC crecieron un 57,7% según la Fiscalía General del Estado. El uso de inteligencia artificial, el engaño digital y la convergencia con economías ilícitas son factores asociados a este incremento. La ciberdelincuencia se ejecuta de forma organizada, repetitiva y orientada al beneficio ilícito. Enfrentarla exige coordinación, continuidad y enfoque preventivo entre Estado y ciudadanía.
- La Fiscalía General del Estado, la Policía Nacional y el Consejo de la Judicatura registran datos coherentes entre sí, lo que permite visualizar el ciclo completo del delito: denuncia, investigación y resolución judicial. El índice de resolución del 78,3% en el Consejo de la Judicatura evidencia una capacidad de respuesta que debe consolidarse con expertos, peritos, protocolos unificados de evidencia digital y formación judicial especializada orientada a anticipar nuevas modalidades de afectación digital.
- El daño de la ciberdelincuencia no termina con la detección del hecho, sino que se extiende a la identidad digital, la salud emocional, la exposición de datos y la reputación de las víctimas. La atención centrada en la víctima debe integrar orientación jurídica, apoyo psicosocial y rutas de reparación, con prioridad para niñas, niños, adolescentes, adultos mayores, personas con discapacidad y ciudadanos con baja alfabetización digital.
- Ecuador cuenta actualmente con instrumentos normativos importantes como la adhesión al Convenio de Budapest, Ley de Ciberseguridad, así como con las unidades especializadas en Fiscalía y Policía Nacional, y participación activa en redes internacionales de ciberinteligencia. El reto es traducir esa base normativa e institucional en tiempos de respuesta más cortos, investigaciones que lleguen a sentencia y acciones de prevención que lleguen a la ciudadanía, fortaleciendo la cultura de prevención y denuncia ante los delitos cometidos mediante las TIC.
- La acción ciudadana prioritaria es detectar, verificar, contener y denunciar. La ciudadanía debe leer antes de hacer clic, revisar remitentes y enlaces, configurar la seguridad de sus cuentas, usar contraseñas diferentes, evitar compartirlas y activar una verificación adicional al inicio de sesión. Si ocurre un incidente, conservar mensajes, capturas, comprobantes, enlaces y números de cuenta aporta elementos útiles para la investigación; reportar el hecho al 1800-DELITO (1800-335486) o ECU911 y presentar la denuncia ante la Fiscalía General del Estado.

# 6. GLOSARIO DE TÉRMINOS

**Ciberdelito / Delito informático**

Conducta ilícita en la que internet o un dispositivo tecnológico actúa como medio o como objeto del delito. En Ecuador, está tipificada en el COIP bajo figuras como la apropiación fraudulenta por medios electrónicos, la violación a la intimidad y el acceso no consentido a sistemas informáticos (28).

**Ingeniería social (Social Engineering)**

Técnica de manipulación psicológica mediante la cual el ciberdelincuente induce a la víctima a revelar información confidencial, transferir dinero o ejecutar acciones dañinas, sin necesidad de vulnerar sistemas informáticos. Explota la confianza, la urgencia o el miedo (40).

**Phishing / Smishing**

Envío masivo de correos electrónicos (phishing) o mensajes de texto (smishing) fraudulentos que simulan ser comunicaciones de bancos, instituciones públicas u otras entidades confiables, con el objetivo de robar credenciales de acceso, datos bancarios o información personal (3).

**Ransomware**

Programa malicioso que cifra los archivos de un dispositivo o red y exige un pago (rescate) para restaurar el acceso. En 2025, este tipo de ataque estuvo implicado en el 44% de las brechas de seguridad a nivel global (41).

**Infostealer (programa que roba información)**

Programa diseñado para extraer de forma silenciosa credenciales, contraseñas, datos financieros e información personal almacenada en dispositivos infectados, y transmitirlos a servidores controlados por delincuentes. Ecuador registró 85.315 detecciones en 2025 (6).

**Enlace con nombre parecido al oficial (typosquatting)**

Registro de un dominio web con una variación ortográfica mínima respecto al dominio oficial de una entidad conocida (ej.: fiscalia-ec.com en lugar de fiscalia.gob.ec), con el propósito de redirigir al usuario a un sitio fraudulento (39).

**Sextorsión**

Modalidad de extorsión en la que el delincuente obtiene material multimedia de contenido íntimo bajo engaño o manipulación afectiva, y posteriormente amenaza a la víctima con difundirlo públicamente si no realiza un pago. Afecta con especial intensidad a adolescentes y jóvenes (42).

**Convenio de Budapest**

Primer tratado internacional sobre ciberdelincuencia, adoptado por el Consejo de Europa en 2001 y abierto a países no miembros. Establece estándares para tipificar delitos informáticos, facilitar la preservación y obtención de evidencia digital transfronteriza y fortalecer la cooperación judicial y policial internacional. Ecuador se adhirió en diciembre de 2024 (43).

**Doble verificación (Doble o Múltiple Factor de Autenticación)**

Mecanismo de seguridad que exige al usuario verificar su identidad mediante al menos dos elementos distintos: algo que sabe (contraseña), algo que posee (teléfono móvil, token) o algo que es (huella dactilar, reconocimiento facial). Dificulta el acceso no autorizado incluso cuando la contraseña ha sido comprometida (34).

# 7. BIBLIOGRAFÍA


1. Juca-Maldonado F, Medina-Peña R. Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. Revista Portal de la Ciencia. 2023; 4(3): p. 325-337 available: https://doi.org/10.51247/pdlc.v4i3.394.

2. Mónica J. Ataques cibernéticos: causas, tipos y consecuencias. [Online].; 2022 [cited 2026 junio. Available from: https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias.

3. Universidad internacional de la Rioja. Delitos Informáticos: Tipos, legislación y medidas de prevención. [Online].; 2024 [cited 2026 junio. Available from: https://ecuador.unir.net/actualidad-unir/delitos-informaticos/.

4. Caja Rural Teruel. Los 12 principales ciberdelitos en el mundo: protégete contra ellos. [Online].; 2024 [cited 2026 junio. Available from: https://www.ruralteruel.com/es/12-principales-ciberdelitos-mundo-protegete-contra-ellos.

5. LISA Institute. Avances de la Ciberseguridad y el Cibercrimen desde la realidad de Ecuador. [Online]. [cited 2026 junio. Available from: https://www.lisainstitute.com/blogs/blog/avances-ciberseguridad-cibercrimen-ecuador?srsltid=AfmBOoo1HQjcYOgyglkDNv-2R8hWRQjBtBpsvApMP_T3UvDd8ttYOCA0.

6. ESET. Robos de información sensible: ¿Cuáles son los 6 infostealers que más afectaron Latinoamérica en 2025? [Online].; 2025 [cited 2026 junio. Available from: https://www.eset.com/ec/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/robos-de-informacion-sensible-cuales-son-los-6-infostealers-que-mas-afectaron-latinoamerica-en-2025/.

7. FBI. Internet Crime Report 2024. Federal Bureau of Investigation; 2025, available to https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

8. INTERPOL. Una operación importante contra la ciberdelincuencia permite detener a 1 006 sospechosos. [Online].; 2024 [cited 2025 06. Available from: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Una-operacion-importante-contra-la-ciberdelincuencia-permite-detener-a-1-006-sospechosos.

9. INTERPOL. 439 millones de dólares estadounidenses recuperados en una operación contra la delincuencia financiera. [Online].; 2025 [cited 2026 junio. Available from: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2025/439-millones-de-dolares-estadounidenses-recuperados-en-una-operacion-contra-la-delincuencia-financiera.

10. Porrúa M, Moncayo G, Paz S, Nowersztern A, Bejarano J, Baudino M, Bordese M, Barret K, Baena C, Jaramillo M, Garces O & Isido A. Informe de ciberseguridad 2025: Desafíos de vulnerabilidad y madurez para cerrar las brechas en América Latina y el Caribe. [Online].; 2025 [cited 2026 junio. Available from: https://doi.org/10.18235/0013872.

11. EUROPOL: Informe de Evaluación de la Amenaza del Crimen Organizado en Internet (IOCTA). [Online].; 2025 [cited 2026 junio. Available from: https://www.dsn.gob.es/es/actualidad/ultima-hora/europol-iocta2025.

12. Kulikova T. Altukhova O, Dedenok R, Kovtun A, Shimko I & Lazaricheva A. El spam y el phishing en 2024. [Online].; 2025 [cited 2026 JUNIO. Available from: https://securelist.lat/spam-and-phishing-report-2024/99599/.

13. Kshetri, N. The global cyber-crime industry: Economic, institutional and strategic perspectives. Springer Science & Business Media. [Online].; 2010. Available from:

https://www.researchgate.net/publication/285998465_The_global_cybercrime_industry_Economic_institutional_and_strategic_perspectives.

14. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2020. European Union Agency for Law Enforcement Cooperation. Europol. [Online].; 2020. Available from: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

15. NTT DATA Cybersecurity. Informe de tendencias y ciberamenazas del segundo semestre de 2025: Departamento de Cyber Threat Intelligence. Departamento de Cyber Threat Intelligence. NTT DATA. https://dam.nttdata.com/api/public/content/Cyber-Threat-Intelligence-Trends-Report-ES-2025-2semestre?v=de392914. 2025.

16. Sánchez Segura C. El impacto social y jurídico de los ciberdelitos más frecuentes en la ciudad de Santiago de Cali, de los años 2018 al 2022. [Online].; 2023. Available from: https://repository.unilibre.edu.co/handle/10901/30275.

17. El Tiempo. Alerta en línea es la nueva estrategia en Bogotá para evitar ciberdelitos. [Online].; 2023. Available from: https://www.eltiempo.com/bogota/ciberdelitos-alerta-en-linea-es-la-nueva estrategia-en-bogota-para-evitar-ciberdelitos-803090.

18. Holt TJ, Bossler AM. Cybercrime and digital forensics: An introduction. 2nd ed.: Routledge.; 2020.

19. Sánchez Segura C. La evolución de la ciberdelincuencia en España: Retos y tendencias actuales. available https://hdl.handle.net/20.500.12880/13770. 2025 junio.

20. Ponemon Institute. Cost of a Data Breach Report 2021. [Online].; 2021. Available from: https://www.ponemon.org/library/cost-of-a-data-breach-report.

21. Wall DS. Cybercrime: The transformation of crime in the information age. Polity.. [Online].; 2007. Available from: https://www.wiley.com/en-ie/Cybercrime:+The+Transformation+of+Crime+in+the+Information+Age-p-9780745627359.

22. Interpol. Informe sobre ciberdelincuencia en las Américas: Tendencias y amenazas emergentes. Lyon: Organización Internacional de Policía Criminal; 2025. Report No.: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ww

w.interpol.int/es/content/download/23674/file/Annual%2520Report%25202024%2520SP.pdf&ved=2ahUKEwjRqPWxy_iUAxXPTTABHb2aOrcQFnoECCIQAQ&usg=AOvVaw2gCnZr5tiPoeGpTcLWEMvW.

23. Centro de Respuesta a Incidentes Informáticos de la Escuela Politécnica Nacional (SIRT-EPN). Phishing con asunto: "Citación legal de la Fiscalía General del Estado". [Online].; 2021 [cited 2026 junio. Available from: https://www.csirt-epn.edu.ec/como-tener/182-phishing-asunto-citacion-legal-fiscalia.

24. Asobanca. Recomendaciones para fortalecer tu seguridad digital en la era de la inteligencia artificial. [Online].; 2024 [cited 2026 junio. Available from: https://asobanca.org.ec/recomendaciones-seguridad-digital/.

25. Ponce M. Delitos informáticos: Caso Ecuador. Revista San Gregorio. 2024 junio; 1(58): p. 119.123, Available from: https://doi.org/10.36097/rsan.v1i58.2667.

26. UNIR. Prevención de Fraudes en Internet: Tipos y estrategias para evitarlos. [Online].; 2025 [cited 2025 junio. Available from: https://ecuador.unir.net/actualidad-unir/prevencion-fraudes/.

27. Superintendencia de Economía Popular y Solidaria. Guía de Señales de Alerta para la Prevención de Lavado de Activos y Financiamiento de delitos como el Terrorismo, En las Entidades del Sector Financiero Popular y Solidario. [Online].; 2024 [cited 206 junio. Available from: https://www.seps.gob.ec/wp-content/uploads/1.1.-Gui%CC%81a-alertas-de-riesgo-PLA.pdf.

28. Presidencia del Ecuador. 2024. Suplemento del Registro Oficial No. 180 , 10 de Febrero 2014. 2014. Available from: https://www.gob.ec/sites/default/files/regulations/2020-09/1.%20COIP.pdf

29. Molina F, Guambo D, Santillán JC, Lozada R. Ciberseguridad en Instituciones Públicas de Chimborazo: Un Diagnóstico Situacional. Tesla Revista Científica. 2025; 5(2): p. Available from: https://doi.org/10.55204/trc.v5i2.e498.

30. Hernández V, Granja S, Arias J. Efectividad de las políticas implementadas para garantizar la seguridad cibernética en Ecuador. Revista Universidad y Sociedad. 2024 octubre 30;: p. Available from:

https://rus.ucf.edu.cu/index.php/rus/article/view/4623/5034.

31. Garcia E, Cuenca JP. Guía de implementación de buenas prácticas de seguridad en redes. Caso de estudio Infocentros MINTEL. Revista Cientifica Dominio de las Ciencias. 2021; 7(4): p. 377 - 398. Available from: https://sga.unae.edu.ec/media/publicacionpersona/2023/05/31/publicacion_20235311647 20.pdf.

32. Santos M. Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento. [Online].; 2022. Available from: https://repositorio.uasb.edu.ec/bitstreams/0e71421e-4fc7-45fc-b48c-2b38eb6eaa3a/download.

33. Fiscalía General del Estado. Resolución No 003 FGE-2023. [Online].; 2023 [cited 2026 junio. Available from: https://www.fiscalia.gob.ec/transparencia/2023/febrero/a3/RESOLUCION-003-FGE-2023.pdf.

34. Unión Internacional de Telecomunicaciones [UIT]. Global Cybersecurity Index 2024. [Online].; 2024. Available from: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.

35. Asobanca. Recomendaciones para fortalecer tu seguridad digital en la era de la inteligencia artificial. [Online].; 2024. Available from: https://asobanca.org.ec/recomendaciones-seguridad-digital/.

36. UNIR. Prevención de Fraudes en Internet: Tipos y estrategias para evitarlos. [Online].; 2025 [cited 2026 junio. Available from: https://ecuador.unir.net/actualidad-unir/prevencion-fraudes/.

37. Asobanca. Recomendaciones para fortalecer tu seguridad digital en la era de la inteligencia artificial. [Online].; 2024 [cited 2026 junio. Available from: https://asobanca.org.ec/recomendaciones-seguridad-digital/).

38. Zambrano A, Loor F, Zambrano W, Párraga R. Delitos informáticos en tiempos de covid: revisión literaria ecuador. [Online]. [cited 2026 junio. Available from:

https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf#.

39. Kaspersky. Typosquatting: definición y explicación. [Online].; 2021 [cited 2026 junio. Available from: https://latam.kaspersky.com/resource-center/definitions/what-is-typosquatting.

40 Jiménez M. Ataques cibernéticos: causas, tipos y consecuencias. PiraniRisk, 2022. Available from: https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias.

41 NTTDATA. *Informe de Amenazas Cibernéticas 2º Semestre 2025. 2026.* Available from: https://mexico.nttdata.com/insights/news/ntt-data-alerta-sobre-un-cambio-de-paradigma-en-las-ciberamenazas

42 Fiscalía General del Estado. Resolución No 041 FGE-2023. [Online].; 2023 [cited 2026 junio. Available from: https://www.fiscalia.gob.ec/transparencia/2023/julio/a3/RESOLUCION-041-FGE-2023.pdf.

43 Presidencia del Ecuador. 2024. Decreto Ejecutivo No. 332 Available from: https://strapi.lexis.com.ec/uploads/DE_332_20240612145331_1_6683002cc1.pdf