

ANÁLISIS DE LA CIBERDELINCUENCIA

BOLETÍN

EN ESTA EDICIÓN

**Conductas delictivas
asociadas al secuestro, la
extorsión, la suplantación
de identidad y el
ciberacoso**

Copyright ©2026



Dirección de Ciberdelitos
Ministerio del Interior

Boletín de Análisis sobre la Ciberdelincuencia: Conductas delictivas asociadas al secuestro,
la extorsión, la suplantación de identidad y el ciberacoso

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, Subrogante

MAGÍSTER JORGE NÉJER GUERRERO

Responsables y Colaboradores

Redacción técnica del documento:

MAGÍSTER GABRIEL REINOSO MARTÍNEZ, Analista de Ciberdelitos

INGENIERO CÉSAR TRELLES SEGOVIA, Analista de Ciberdelitos

INGENIERO FABIÁN SILVA TOLEDO, Analista de Ciberdelitos

Revisión técnica del documento:

INGENIERO FREDDY GALLARDO SOSA, Especialista de Ciberdelitos

Redacción y compilación:

MAGÍSTER CARLOS SIMBAÑA COBA, Analista de Ciberdelitos

Edición y Adaptación:

MAGÍSTER DUVAL MONTATIXE CAIZALUISA, Analista de Ciberdelitos

SEPTIEMBRE, 2026



EL NUEVO
ECUADOR

Ministerio del Interior

CONTENIDO

SÍNTESIS DEL BOLETÍN	5
INTRODUCCIÓN	6
Alcance.....	7
Objetivos	7
Objetivo General:	7
Objetivos Específicos:.....	7
TECNOLOGÍAS Y DINÁMICAS DEL DELITO	8
Dinámica del delito	9
ANÁLISIS DE LAS CONDUCTAS DELICTIVAS	10
Secuestro facilitado mediante tecnologías.....	10
Extorsión mediante medios digitales	11
Suplantación de identidad	12
Ciberacoso	12
PERFILAMIENTO DE CONDUCTAS DELICTIVAS Y PATRONES DE COMPORTAMIENTO EN ECUADOR	13
Aportes de los avances tecnológicos y el análisis de datos para la prevención del delito.....	13
Los patrones de comportamiento como dimensión esencial en el perfilamiento criminal	14
Contexto ecuatoriano: los patrones de comportamiento frente a la transformación del fenómeno delictivo	15
Hacia un modelo integral de análisis criminal para la prevención del delito en Ecuador ..	16
ESCALAMIENTO Y VALORACIÓN DEL RIESGO.....	17
VÍCTIMAS, FACTORES DE VULNERABILIDAD Y SEÑALES DE ALERTA.....	22
Víctimas y sus perfiles	22
Secuestro	22
Extorsión	22
Suplantación de identidad	23
Ciberacoso.....	23



Factores de vulnerabilidad.....	23
Factores tecnológicos y de información.....	23
Factores personales y relacionales.....	23
Factores sociales y de vulnerabilidad	24
Impacto y afectaciones en las víctimas	24
Señales de alerta.....	24
PANORAMA ESTADÍSTICO	25
Casos documentados en el Ecuador	25
Dos sentenciados como cómplices de secuestro extorsivo	26
El medio digital Eco Amazónico sufrió una suplantación de identidad en Facebook	26
Estadísticas del fenómeno estudiado.....	27
Fiscalía General del Estado	27
Consejo de la Judicatura	27
MEDIDAS DE PREVENCIÓN Y RESPUESTA INSTITUCIONAL	28
Recomendaciones multisectoriales de prevención y mitigación del riesgo	29
Directrices de implementación por sector	29
Ejes técnicos y operativos.....	33
Verificación de identidad y reducción de huella digital	33
Fortalecimiento de cuentas y preservación de evidencia digital.....	34
Gestión de amenazas y protección de víctimas	34
Mecanismos de articulación interinstitucional.....	34
Acciones cuando existe riesgo para la vida.....	35
CONCLUSIONES	36
GLOSARIO DE TÉRMINOS.....	37
BIBLIOGRAFÍA	39



SÍNTESIS DEL BOLETÍN

La expansión de los entornos digitales ha transformado las dinámicas de diversas conductas delictivas en el Ecuador. El uso de redes sociales, servicios de mensajería, herramientas de inteligencia artificial, técnicas de ingeniería social y mecanismos que dificultan la identificación de los responsables ha ampliado las posibilidades de aproximación, engaño, intimidación y coerción sobre las víctimas. En este escenario, el ciberespacio puede constituirse en un medio para la obtención de información, el contacto con potenciales víctimas, la ejecución o facilitación de determinadas conductas delictivas y, en ciertos casos, la preparación de acciones que posteriormente trascienden al entorno físico.

Frente a esta realidad, el presente boletín aborda las conductas delictivas asociadas al secuestro, la extorsión, la suplantación de identidad y el ciberacoso, desde una perspectiva multidisciplinaria que integra elementos criminológicos, investigativos, tecnológicos, estadísticos y jurídicos. El análisis busca contribuir a la comprensión de las dinámicas mediante las cuales los medios digitales pueden ser utilizados para facilitar estas conductas, así como identificar factores de riesgo y elementos que fortalezcan las capacidades de prevención y respuesta institucional.

El análisis permitió identificar patrones relacionados con la obtención de información mediante fuentes abiertas (OSINT), aproximación y contacto con potenciales víctimas, generación de confianza o engaño, intimidación, coerción y escalamiento de las amenazas. Asimismo, se analizaron modalidades que incorporan el uso de medios digitales, entre ellas la suplantación de identidad, la utilización de contenidos manipulados o generados mediante inteligencia artificial —incluidos los deepfakes—, las exigencias económicas o “vacunas” comunicadas mediante servicios de mensajería, la sextorsión y el empleo de información obtenida en entornos digitales que puede facilitar la planificación de otras conductas delictivas.

Desde el componente criminológico se analizaron comportamientos, formas de aproximación, mecanismos de presión, posibles motivaciones, utilización de tecnologías y patrones de escalamiento de las amenazas, considerando la interacción existente entre el entorno digital y las posibles consecuencias en el entorno físico. Este enfoque permite comprender que determinadas conductas pueden iniciar mediante interacciones digitales y evolucionar hacia escenarios de mayor riesgo para la víctima.

En el ámbito jurídico, se desarrolló un análisis de las conductas objeto de estudio y de su tratamiento dentro del marco normativo ecuatoriano, particularmente respecto del secuestro, la extorsión, la suplantación de identidad y el ciberacoso, considerando las disposiciones



EL NUEVO
ECUADOR

Ministerio del Interior

aplicables del Código Orgánico Integral Penal (COIP). Este componente se complementó con la identificación de factores de vulnerabilidad y la formulación de medidas preventivas dirigidas a distintos sectores, orientadas a reducir la exposición al riesgo y fortalecer la capacidad de respuesta frente a posibles hechos delictivos.

El componente estadístico consideró información proveniente de los registros de denuncias de la Fiscalía General del Estado (FGE) y de las causas judiciales del Consejo de la Judicatura, con el propósito de analizar el comportamiento de las conductas estudiadas e identificar patrones de incidencia territorial y otros elementos relevantes para su comprensión.

Los resultados analizados resaltan la importancia de fortalecer la articulación interinstitucional entre el Servicio Integrado de Seguridad ECU 911, la Policía Nacional a través de sus unidades especializadas, la Fiscalía General del Estado, las instituciones competentes y los proveedores de tecnología y servicios digitales, especialmente en aquellos casos que requieran una respuesta coordinada y la adecuada preservación de evidencia digital.

Finalmente, resulta relevante fortalecer y estandarizar los canales de denuncia, mejorar la interoperabilidad y consolidación de la información estadística y operativa, así como impulsar acciones permanentes de prevención y concientización ciudadana. La adopción de prácticas de ciberseguridad, mecanismos de verificación de identidad y medidas de protección de la información personal puede contribuir a reducir factores de vulnerabilidad y fortalecer una cultura digital responsable, preventiva y resiliente frente a las nuevas dinámicas delictivas.

INTRODUCCIÓN

El avance tecnológico y la hiperconectividad han transformado las dinámicas sociales, económicas y culturales. Esa misma evolución ha sido aprovechada por la delincuencia contemporánea, sofisticando la ejecución de conductas como la extorsión, la suplantación de identidad, el ciberacoso y las fases logísticas preparatorias del secuestro.

Frente a un escenario donde el ciberespacio desvanece las fronteras físicas, la respuesta institucional exige superar los enfoques reactivos tradicionales. Por ello, este boletín se articula en torno al análisis experto y al perfilamiento de conductas delictivas en el Ecuador y la región. Mediante un enfoque multidisciplinario que integra la criminología, psicología, ciberinteligencia, el contexto normativo contemporáneo y la informática forense, esta edición examina tanto el modo de operar tecnológico como las motivaciones, patrones de comportamiento y vulnerabilidades de las víctimas que moldean el fenómeno delictivo en la era digital.

Alcance

- **Patrones de conductas delictivas:** Análisis de las formas de contacto, engaño, presión y manipulación que utilizan los responsables de estas conductas en entornos digitales.
- **Ámbito delictivo y uso de las tecnologías:** Cobertura de conductas como la extorsión digital, la suplantación de identidad, el ciberacoso y la recopilación de información táctica mediante fuentes abiertas para la facilitación de extorsiones, secuestros o reclutamiento de menores; potenciadas por herramientas de inteligencia artificial (IA).
- **Contexto legal y desafíos normativos:** Evaluación de la legislación vigente y los estándares internacionales frente a la rápida evolución de la tecnología, identificando vacíos jurídicos y retos en la admisibilidad de la evidencia digital.
- **Enfoque multidisciplinario integral:** Articulación del análisis de conducta, el marco legal, la investigación digital y la protección de las personas afectadas.
- **Ciclo completo de gestión de amenazas:** Comprende acciones para anticipar riesgos, conservar información útil, investigar los hechos y apoyar la actuación de las autoridades competentes para asegurar una judicialización efectiva.

Objetivos

Objetivo General:

Proporcionar un marco analítico, estratégico y multidisciplinario sustentado en el análisis de las conductas delictivas y de su contexto legal y tecnológico para fortalecer las capacidades de prevención, neutralización y judicialización de la ciberdelincuencia en la sociedad contemporánea.

Objetivos Específicos:

- Describir los patrones de contacto, presión y comportamiento asociados a quienes ejecutan extorsiones, suplantaciones de identidad, ciberacoso y acciones preparatorias de secuestro mediante medios digitales.
- Analizar el impacto de las tecnologías emergentes como la inteligencia artificial en el cometimiento de ciberdelitos y sus consecuencias en la seguridad ciudadana.
- Fortalecer el conocimiento de la ciudadanía sobre las señales de alerta que permitan identificar oportunamente intentos de engaño, intimidación, suplantación o

manipulación mediante medios digitales, así como las acciones de prevención y respuesta frente a estas conductas

- Identificar estrategias y posibles acciones interinstitucionales que permitan anticipar la amenaza, reducir la vulnerabilidad victimal y proteger la integridad de los ciudadanos e instituciones.

TECNOLOGÍAS Y DINÁMICAS DEL DELITO

Las tecnologías de comunicación, interacción, localización y pago pueden intervenir de manera transversal en distintas fases de una conducta delictiva. En los casos y fuentes revisados para Ecuador, su uso se observa en la obtención de información, el acercamiento inicial, la creación de credibilidad, la intimidación, el seguimiento y la coordinación de acciones presenciales. A continuación, se describe su función operativa y la secuencia general identificada:

Tabla 1
Tecnologías y Dinámicas Del Delito

Tecnologías y Dinámicas Del Delito	
Tecnología	Uso identificado en Ecuador
Redes sociales, mensajería instantánea y plataformas digitales	Facilitan la consulta de información pública, el establecimiento de contacto y la coordinación de interacciones. En Ecuador se han documentado amenazas por WhatsApp desde centros de privación de libertad y solicitudes falsas de transporte o flete utilizadas para concertar encuentros con las víctimas (FGE, 2026b, 2026e, 2026g; MDI, 2025).
Llamadas, videollamadas y servicios de voz por internet	Permiten ejercer presión en tiempo real, transmitir amenazas y sostener comunicaciones directas con la víctima o su entorno. En Ecuador se ha reportado su empleo, desde el interior de los centros de privación de libertad, para coordinar extorsiones (Asamblea Nacional del Ecuador, 2026).
Perfiles falsos, cuentas suplantadas y contenidos manipulados	Se emplean para ocultar o aparentar identidades, reforzar la credibilidad de una comunicación y sostener interacciones engañosas. Las herramientas de inteligencia artificial permiten generar voz, imagen o video sintéticos, recursos identificados como facilitadores de suplantación y extorsión (MDI, 2024).
Bases de datos filtradas y herramientas de geolocalización	La información personal expuesta o procedente de filtraciones puede utilizarse para perfilar objetivos, personalizar mensajes y aumentar la credibilidad del contacto. La ubicación en tiempo real, los rastreadores GPS y las ubicaciones compartidas mediante mensajería pueden facilitar el seguimiento de movimientos o la coordinación de encuentros (MDI, 2024; UNODC, s.f.; FGE, 2026g).

Medios de pago	Las exigencias económicas pueden canalizarse mediante transferencias, depósitos y cuentas de terceras personas que reciben o movilizan fondos. También se ha documentado el intento de uso de aplicaciones bancarias instaladas en el dispositivo de la víctima para transferir dinero (FGE, 2024, 2026d, 2026e).
Mecanismos de anonimización	En fuentes nacionales se reporta el uso de chips internacionales, roaming y dispositivos móviles ingresados irregularmente a centros de privación de libertad, junto con cuentas o perfiles orientados a ocultar la identidad de quien opera el canal digital (Asamblea Nacional del Ecuador, 2026; FGE, 2026f; MDI, 2025). Las herramientas orientadas a ocultar la identidad digital dificultan la identificación del responsable (Salazar Méndez, 2021).

Elaboración: Dirección de Ciberdelitos – Ministerio del Interior.

Dinámica del delito

El esquema organiza funciones observadas en las fuentes revisadas, desde la obtención de información y el contacto inicial hasta el seguimiento y una posible articulación con acciones presenciales. La secuencia es referencial y puede variar según las características de cada caso.

Recopilación de información → Selección → Aproximación → Generación de confianza → Manipulación e intimidación → Vigilancia y control → Posible paso al espacio físico.

Recopilación de información. La obtención inicial de datos puede apoyarse en perfiles públicos, conversaciones iniciadas desde números desconocidos, ofertas falsas publicadas en plataformas y herramientas que reúnen información de una misma persona en distintos servicios digitales (MDI, 2024, 2025). Los datos obtenidos pueden incluir fotografías, ubicación, información familiar y referencias de contacto.

Selección. La información recopilada permite priorizar objetivos y adaptar el canal de aproximación. Entre los elementos observados constan la actividad económica visible, la oferta de bienes o servicios en plataformas y la disponibilidad de datos que facilitan ubicar o contactar a la persona (MDI, 2025; FGE, 2026b, 2026f, 2026g).

Aproximación y generación de confianza. El contacto puede presentarse como una relación comercial, laboral, social, afectiva o lúdica (juegos, actividades recreativas, etc.). La interacción sostenida, la afinidad aparente y, en algunos entornos, la oferta de recompensas o dinero pueden utilizarse para fortalecer el vínculo y obtener mayor interacción de la persona objetivo (MDI, 2025).

Manipulación e intimidación. La información obtenida en fases previas puede utilizarse para personalizar engaños y aumentar la credibilidad del mensaje. La intimidación adquiere mayor



EL NUEVO
ECUADOR

Ministerio del Interior

capacidad de presión cuando incorpora referencias verificables al domicilio, lugar de trabajo o entorno cercano de la víctima (MDI, 2025; FGE, 2026c).

Vigilancia y control. El seguimiento digital puede combinarse con la observación del entorno físico. Muchos delincuentes mantienen el uso reiterado de tecnologías para estudiar desplazamientos y el envío de imágenes o videos de domicilios y negocios como evidencia de conocimiento del entorno (UNODC, s.f.; FGE, 2026f).

Posible paso al espacio físico. Los canales digitales pueden facilitar la coordinación de encuentros, la remisión de ubicaciones y la identificación de lugares de interés. En casos documentados en Ecuador, el contacto iniciado mediante plataformas digitales derivó en encuentros presenciales, visitas intimidatorias o privaciones de libertad de la víctima asociadas a encuentros coordinados por medios digitales (FGE, 2026b, 2026c, 2026g).

El valor analítico de esta secuencia radica en mostrar la continuidad funcional entre datos, comunicaciones y acciones presenciales. Las etapas pueden presentarse de manera parcial, simultánea o en un orden diferente, según las características de cada caso. Por ello, cada señal de alerta detectada en una fase temprana (por ejemplo, un contacto desconocido que conoce datos personales) es una oportunidad de interrumpir el ciclo antes de que avance hacia la coerción o el contacto físico.

ANÁLISIS DE LAS CONDUCTAS DELICTIVAS

Las conductas examinadas corresponden a categorías penales distintas, algunas atacan directamente bienes y sistemas digitales, mientras otras son infracciones tradicionales potenciadas por tecnologías de información y comunicación. En ambos casos, la calificación jurídica debe partir del bien jurídico afectado, la conducta ejecutada, la finalidad y el resultado, antes que del canal empleado. La tecnología puede operar como instrumento, entorno de interacción, fuente de información o medio para ocultar la identidad; aun así, cada tipo penal conserva íntegros los elementos que exige. Estudios especializados describen, además, el uso creciente de inteligencia artificial, datos sustraídos y servicios digitales para potenciar el engaño y la manipulación de las personas, ampliando el alcance delictivo (Europol, 2024).

Secuestro facilitado mediante tecnologías

De acuerdo con los artículos 161.- secuestro y 162.- Secuestro extorsivo del COIP, existe secuestro cuando una persona es privada de su libertad, retenida, ocultada, arrebatada o trasladada contra su voluntad. El secuestro será extorsivo cuando, además, se persiga cometer otra infracción u obtener dinero, bienes, beneficios, acciones u omisiones a cambio de su

libertad. Los medios digitales pueden facilitar la selección de la víctima mediante información pública, el conocimiento de rutinas y vínculos familiares, la coordinación entre participantes, la vigilancia o la transmisión de exigencias. Estos medios pueden facilitar la conducta, aunque el secuestro requiere que exista una privación real de la libertad de la víctima (Asamblea Nacional del Ecuador, 2014).

Esta conducta debe diferenciarse del denominado secuestro virtual, modalidad en la que se comunica falsamente que una persona ha sido retenida. Para reforzar el engaño, se utilizan datos personales, presión temporal, voces imitadas o imágenes manipuladas como supuesta prueba de vida. El FBI ha advertido el empleo de fotografías obtenidas de redes sociales y alteradas para respaldar exigencias de rescate sin que exista un secuestro real (Federal Bureau of Investigation-FBI, 2025). Cuando no existe una privación real de la libertad, los hechos pueden corresponder al delito de extorsión previsto en el artículo 185.- Extorsión del COIP, siempre que concurren intimidación, exigencia y perjuicio económico. Por su parte, el artículo 163 del COIP regula la simulación de secuestro, que se configura cuando una persona finge estar secuestrada, supuesto distinto de una falsa comunicación realizada por terceros.

Extorsión mediante medios digitales

El artículo 185.- Extorsión del COIP establece que la violencia o intimidación puede ejecutarse por cualquier medio, incluidos los digitales o electrónicos. La conducta comprende la exigencia de hacer u omitir un acto, efectuar pagos, entregar bienes o facilitar información con el propósito de obtener un beneficio y causar un perjuicio económico. En el entorno digital se manifiesta mediante mensajería instantánea, llamadas, perfiles falsos o cuentas de otras personas tomadas sin autorización y amenazas de violencia, exposición de información, daño a la reputación o divulgación de contenido privado. La disponibilidad de datos personales y el uso de herramientas de inteligencia artificial permiten personalizar los mensajes aumentando su credibilidad ante la víctima (Europol, 2024).

La extorsión sexual requiere un análisis específico. Cuando, mediante violencia, amenazas o chantaje, se induce, incita u obliga a una persona a exhibir su cuerpo desnudo, semidesnudo o en actitudes sexuales para obtener un provecho personal o para un tercero, puede configurarse el delito de extorsión sexual previsto en el artículo 172.1 del COIP. Si se revela o divulga a terceros contenido digital, mensajes, correos, imágenes, audios, videos u otro contenido íntimo de carácter sexual contra la voluntad de la persona, puede aplicarse lo establecido en el artículo 179.- Revelación de secreto o información personal de terceros del COIP. Por otra parte, el artículo 178, relativo a la violación a la intimidad, puede resultar aplicable cuando el contenido

privado haya sido obtenido mediante acceso, interceptación, grabación u otros medios sin consentimiento o autorización legal. Cuando el contenido haya sido obtenido ilícitamente y posteriormente divulgado, cada conducta deberá analizarse de acuerdo con las circunstancias del caso.

Suplantación de identidad

El artículo 212 del COIP sanciona a quien suplanta la identidad de otra persona para obtener un beneficio propio o de un tercero, en perjuicio de la persona suplantada. Por tanto, la sola semejanza entre perfiles resulta insuficiente para determinar una suplantación: debe existir el uso de una identidad ajena para obtener un beneficio y causar un perjuicio. Las modalidades comprenden la toma de control de cuentas, la clonación de perfiles, el uso de documentos o datos sustraídos y la generación de voz, imagen o video mediante inteligencia artificial para aparentar una identidad real. Europol identifica la apropiación de cuentas y los contenidos generados artificialmente como recursos utilizados para hacer más creíbles los engaños y la manipulación de las personas (Europol, 2024).

La suplantación de identidad también puede utilizarse para facilitar otros delitos. Por ejemplo, puede servir para engañar a una persona y obtener dinero, generar información falsa o acceder sin autorización a cuentas o información. Entre las principales señales de alerta se encuentran los avisos de acceso desconocido, cambios inesperados de contraseñas, duplicación de perfiles, solicitudes urgentes de dinero o información desde medios de contacto diferentes a los habituales y comunicaciones cuya voz o imagen generen dudas y requieran verificar la identidad de la persona por otro medio.

Ciberacoso

El término ciberacoso comprende distintas conductas realizadas mediante medios digitales y su valoración jurídica depende de las características de cada caso. El artículo 154.2.- Hostigamiento del COIP sanciona el hostigamiento cuando una persona, mediante tecnologías u otros medios, molesta, perturba o angustia de forma insistente o reiterada y busca acercarse a la víctima con la finalidad de causarle daño físico o sexual. Dependiendo de los hechos, también pueden presentarse conductas relacionadas con acoso sexual mediante tecnologías, contacto con finalidad sexual con menores, violencia psicológica en relaciones familiares, violación a la intimidad, divulgación de contenido íntimo sin consentimiento o calumnia. La valoración de cada caso debe considerar la frecuencia de las conductas, su finalidad, la relación entre las personas involucradas y la afectación producida (Asamblea Nacional del Ecuador, 2014).

La literatura especializada describe como patrones frecuentes el contacto reiterado e indeseado por redes, correo o mensajería, el acceso a cuentas, el seguimiento de ubicación, la suplantación y el contacto o las amenazas dirigidas a familiares o amistades. También advierte que las conductas digitales y presenciales suelen combinarse (Kaur et al., 2021). El riesgo aumenta cuando el hostigamiento se extiende a varias plataformas, persiste después del bloqueo, incorpora información sobre rutinas o ubicación, amenaza a terceros o pasa de la observación virtual a la presencia física.

PERFILAMIENTO DE CONDUCTAS DELICTIVAS Y PATRONES DE COMPORTAMIENTO EN ECUADOR

Mgs. Johselyn Patricia Espinoza Avilés

Abogada Especialista en Derecho Penal y Criminología, Magíster en Derecho Penal y

Criminología, Master en Género y Desarrollo Profesional

Profesora y Directora de Trabajos de Investigación en la Universidad de La Rioja, España.

Aportes de los avances tecnológicos y el análisis de datos para la prevención del delito

La perfilación criminal, también denominada criminal profiling, constituye una técnica especializada en el ámbito de la psicología criminal orientada a la elaboración de hipótesis acerca de las características del autor desconocido de un hecho delictivo. Su aplicación parte del análisis sistemático de la información disponible sobre el delito, incluyendo elementos relativos a la escena del crimen, la conducta desplegada por el autor durante su comisión y las características de la víctima. A partir de la integración e interpretación de estos indicadores, se establecen inferencias que permiten formular un perfil aproximado del posible responsable. En este sentido, la perfilación criminal no pretende identificar de manera directa al autor, sino aportar información que contribuya a delimitar el universo de posibles sospechosos y a orientar las líneas de investigación policial y criminalística.

El desarrollo del perfilamiento criminal puede entenderse a partir de diferentes enfoques que muestran la progresiva incorporación de herramientas científicas y tecnológicas al análisis del delito.

Entonces, el análisis de la conducta criminal constituye un ámbito de estudio más amplio que trasciende la aplicación de una técnica concreta. Su finalidad es comprender la dinámica delictiva a partir del análisis sistemático, lógico y fundamentado de las conductas que



EL NUEVO
ECUADOR

Ministerio del Interior

intervienen en un hecho delictivo. Este análisis contempla no solo el comportamiento del autor, sino también el de la víctima y, cuando resulte pertinente, el de otros actores presentes en el contexto delictivo, como los testigos. De este modo, permite abordar el hecho criminal desde una perspectiva integral, atendiendo a las interacciones y circunstancias que pueden contribuir a explicar cómo se desarrolla el delito.

Por tanto, el avance tecnológico ha aumentado considerablemente la capacidad de procesamiento de información en las investigaciones criminales. Sin embargo, la incorporación de estas herramientas exige establecer límites jurídicos y mecanismos de control que eviten que la tecnología sustituya injustificadamente la valoración humana. En consecuencia, la evolución tecnológica no elimina la intervención humana, sino que permite complementar la experiencia del investigador con información cuantificable y patrones obtenidos mediante el procesamiento de datos.

Los patrones de comportamiento como dimensión esencial en el perfilamiento criminal

Un patrón de comportamiento puede concebirse como un conjunto de características, acciones o secuencias conductuales que presentan un grado de recurrencia o similitud en uno o varios hechos delictivos. Su identificación requiere analizar de manera conjunta variables relacionadas con la selección de la víctima, el lugar y momento de comisión, la forma de aproximación, las estrategias de interacción, el método empleado durante la ejecución del delito y las conductas posteriores al hecho. La relevancia de estos elementos no reside únicamente en su presencia individual, sino en la relación que mantienen entre sí y en la posibilidad de que su repetición permita reconocer una determinada dinámica delictiva.

Desde esta perspectiva, el comportamiento criminal no debe analizarse como una sucesión de acciones aisladas, sino como un proceso en el que intervienen decisiones, oportunidades, características del entorno y relaciones entre los distintos actores involucrados. El estudio de estas variables permite aproximarse a la lógica mediante la cual se desarrolla un hecho delictivo y, cuando existen elementos suficientes, establecer conexiones entre acontecimientos aparentemente independientes. La investigación reciente sobre crime linkage muestra precisamente que las características conductuales, temporales y espaciales pueden emplearse para valorar la posible vinculación entre delitos, mediante procedimientos que van desde el juicio experto hasta métodos estadísticos y de aprendizaje automático (Burrell et al., 2024), es decir lo que nosotros llamamos el “modus operandi”.

Así podríamos describir la conducta del investigador en los siguientes pasos lógico entre ambos procesos **primero**, observación de la conducta, **segundo**, identificación de



EL NUEVO
ECUADOR

Ministerio del Interior

regularidades, interpretación de los patrones y **tercero**, formulación de hipótesis sobre el posible autor. Así, determinadas características de la actuación delictiva pueden proporcionar información acerca de las decisiones adoptadas, los conocimientos necesarios, las oportunidades aprovechadas o las estrategias empleadas durante la comisión del hecho.

Los patrones deben ser interpretados dentro del contexto específico de cada investigación y contrastados con otras fuentes de evidencia. De este modo, su utilidad reside fundamentalmente en generar hipótesis investigativas susceptibles de ser verificadas mediante procedimientos independientes. La incorporación tecnológica amplía la capacidad analítica, pero no elimina la necesidad de interpretación profesional, control jurídico y supervisión humana.

Contexto ecuatoriano: los patrones de comportamiento frente a la transformación del fenómeno delictivo

En el contexto ecuatoriano, el análisis de los patrones de comportamiento adquiere especial relevancia ante la transformación y diversificación de las dinámicas criminales registradas durante los últimos años. El fenómeno delictivo ha dejado de manifestarse únicamente a través de hechos aislados para evidenciar estructuras y relaciones asociadas con economías ilícitas, disputas territoriales, narcotráfico, extorsión, tráfico de armas, lavado de activos y otras actividades conexas.

Esta transformación plantea un desafío para la investigación criminal: comprender la conducta delictiva más allá de la individualidad de cada caso. En este sentido, el contexto ecuatoriano demanda fortalecer una perspectiva de análisis criminal orientada a identificar relaciones, recurrencias y variaciones en el comportamiento delictivo.

El desafío institucional consiste, por tanto, en desarrollar capacidades que permitan integrar información procedente de distintas fuentes y convertirla en conocimiento útil para la investigación.

Bajo esta perspectiva, **el contexto ecuatoriano justifica la incorporación progresiva de herramientas de análisis de datos, inteligencia criminal e inteligencia artificial**, capaces de procesar grandes volúmenes de información y detectar relaciones que podrían no resultar evidentes mediante el análisis convencional. La tecnología, sin embargo, no sustituye el razonamiento del investigador: su verdadero valor reside en ampliar la capacidad humana para identificar regularidades, generar hipótesis y orientar la investigación sobre bases metodológicamente sustentadas.



EL NUEVO
ECUADOR

Ministerio del Interior

Hacia un modelo integral de análisis criminal para la prevención del delito en Ecuador

La evolución del perfilamiento criminal permite comprender que el análisis de la conducta delictiva no puede limitarse al estudio aislado de un hecho o a la elaboración de una descripción aproximada de un posible autor. La investigación contemporánea ha avanzado hacia modelos que integran variables conductuales, espaciales, temporales y contextuales con el propósito de identificar regularidades y posibles relaciones entre diferentes acontecimientos. En este proceso, el análisis de patrones de comportamiento adquiere especial relevancia, pues permite transformar la información dispersa de múltiples investigaciones en conocimiento útil para comprender la dinámica del delito.

En este sentido, el futuro del análisis criminal en Ecuador debería orientarse hacia un modelo integral y de prevención, capaz de articular el conocimiento criminológico, la experiencia investigativa y las nuevas capacidades tecnológicas. El futuro del análisis criminal en Ecuador debería orientarse hacia un modelo integral y de prevención, capaz de articular el conocimiento criminológico, la experiencia investigativa y las nuevas capacidades tecnológicas.

El proceso puede comprenderse como una secuencia lógica: recopilar información, identificar patrones, analizar relaciones, formular hipótesis, contrastarlas y convertir los resultados en conocimiento para la investigación y la prevención del delito. Cada etapa requiere criterios metodológicos y profesionales que permitan distinguir entre una coincidencia circunstancial y una regularidad verdaderamente significativa.

En definitiva, el perfilamiento criminal, el análisis de patrones de comportamiento y las nuevas tecnologías deben comprenderse como componentes de un mismo proceso orientado a generar conocimiento sobre el fenómeno delictivo. Su mayor aporte no reside únicamente en explicar lo que ocurrió, sino en proporcionar elementos que permitan comprender cómo, dónde, cuándo y bajo qué circunstancias se transforma la conducta criminal. En un contexto como el ecuatoriano, esta capacidad puede contribuir a pasar de una respuesta predominantemente reactiva hacia estrategias de prevención sustentadas en información, análisis y evidencia.

ESCALAMIENTO Y VALORACIÓN DEL RIESGO

PhD. Efrén Ernesto Guerrero Salgado

Abogado especialista en Derechos Humanos, Dr. en Gobierno y Administración Pública,

Profesor Titular de la Pontificia Universidad Católica del Ecuador

El sistema procesal ecuatoriano es acusatorio, y esto tiene una consecuencia importante en el manejo del concepto de verdad. Ontológicamente, no se sostiene en una verdad basada en la subjetividad de los operadores del proceso penal, sino en la existencia de una verdad sustentada en prueba (Starace, 2026). Esta diferencia genera una ruptura respecto de la impunidad manifiesta que pueden producir los sistemas inquisitivos, en los cuales el concepto de verdad se basaba principalmente en el testimonio. El cambio no es solamente procedimental: afecta la manera en que se conocen los hechos y se justifican las decisiones.

El delito digital ya no deja únicamente huellas físicas. El aumento de los delitos relacionados con entornos digitales, así como la utilización de herramientas digitales para cometerlos, se ha intensificado especialmente después de los años de pandemia. Entre los tipos más reportados se encuentran el phishing, el spoofing, la extorsión y los esquemas de inversión fraudulenta (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2022, p.28). Sus víctimas incluyen personas afectadas por la brecha digital, particularmente mayores de sesenta años. La transformación del entorno delictivo obliga, en consecuencia, a revisar las formas de investigación y los instrumentos utilizados para comprenderlo.

Desde esta perspectiva, perfilar y generar hipótesis criminológicas en el espacio digital implica un cambio importante en cómo concebimos el derecho penal y su aplicación práctica en torno a la protección de derechos. La pregunta no consiste únicamente en determinar qué puede hacer una herramienta tecnológica, sino en establecer en qué condiciones sus resultados pueden incorporarse legítimamente a una investigación penal (Martineau et al., 2023, p. 453). Esto se debe a que la capacidad de procesar información no elimina las exigencias de prueba, contradicción y control que caracterizan a un sistema acusatorio, enfrentados a las tecnologías de agentes de inteligencia artificial.

La primera idea es que la inteligencia artificial no constituye un sistema oracular (Véliz, 2026). Es parte de un proceso de recogida y análisis de datos, integrado en el marco más amplio del proceso penal. Por tanto, corresponde pasar de la intuición criminológica a una analítica responsable. El perfilamiento criminal digital solo es legítimo si funciona dentro de un Estado de



EL NUEVO
ECUADOR

Ministerio del Interior

Derecho, respeta la Constitución y el control de convencionalidad, y se presenta como una hipótesis investigativa verificable, no como una etiqueta automática de peligrosidad (Corte Constitucional del Ecuador, 2022, párrs. 40–61). Esta distinción resulta fundamental para abordar los sesgos algorítmicos: los errores de concepción o diseño del sistema de IA.

Esto significa que el perfilamiento no debe concentrarse exclusivamente en la pregunta de quién lo hizo. También debe identificar qué patrones de infraestructura, lenguaje y oportunidad se repiten. En este punto surge la importancia del perfilamiento criminal digital y su relación con la inteligencia artificial. No partimos de un escenario en el que la prueba o el peritaje digitales sean desconocidos: estos mecanismos se han utilizado durante casi dos décadas. La diferencia reside en que la inteligencia artificial amplía las capacidades de analítica de información y de correlación de datos mediante la identificación de patrones (Subrahmanyam, 2026).

Hay que insistir, entonces, en que el perfilamiento criminal digital no es una sentencia anticipada. (Subramaniam, 2026, p. 146). Puede incluir el procesamiento de huellas digitales, logs, direcciones IP, metadatos, wallets, dominios y dispositivos. Asimismo, puede incorporar información sobre modus operandi, cadenas de ataques, tipos de víctimas, horarios e idiomas. La alimentación y el aprendizaje de la máquina permiten relacionar estos elementos y construir firmas conductuales, a partir de las cuales se generan hipótesis relevantes para la investigación penal.

Por ello, el perfilamiento debe entenderse como un proceso técnico-jurídico que integra evidencia digital, patrones criminológicos y análisis de contextos y datos para construir hipótesis sobre autoría, participación, infraestructura de riesgo y continuidad delictiva. Su finalidad es priorizar líneas de investigación, conectar casos y orientar medidas de protección. No puede reemplazar la prueba, justificar formas de vigilancia masiva prohibidas por los estándares constitucionales e interamericanos ni etiquetar a las personas por sus rasgos. La utilidad investigativa del perfil depende, precisamente, de que estos límites permanezcan operativos.

Las herramientas existentes para la perfilación en el ciberespacio intervienen en distintos ámbitos. Entre ellos se encuentran la inteligencia de señales y la inteligencia social basada en redes, foros, dominios y huellas públicas, así como el examen de logs, tráfico y alertas. Sin embargo, disponer de esas fuentes no resuelve por sí mismo el problema. Es necesario analizar las posibilidades del perfilamiento y definir cómo debe funcionar su articulación con la inteligencia artificial. La pregunta por el alcance técnico debe acompañarse siempre de una pregunta por sus condiciones jurídicas de utilización.

Además, la inteligencia artificial actúa como un acelerador en ambos lados: tanto para los delincuentes como para las fuerzas y cuerpos de seguridad de los Estados. El informe de inteligencia de Anthropic (2026) muestra el incremento del uso de estas tecnologías para potenciar engaños cada vez más sofisticados. Al mismo tiempo, aumenta la dificultad estatal para encontrar huellas, por la complejidad de los mecanismos de criptografía y de gestión de la prueba. No estamos, por tanto, ante una herramienta cuyo aprovechamiento se encuentre reservado a quienes investigan el delito.

En la investigación, la inteligencia artificial puede utilizarse para el triaje de alertas, la detección de anomalías, el clustering, el análisis de lenguaje, la revisión de evidencia y la visualización de redes. Del lado delictivo, permite desarrollar phishing personalizado, clonación de voz, deepfakes, documentos sintéticos, malware asistido, inyección de prompts y automatización de la explotación y la evasión.

El problema central no consiste simplemente en usar inteligencia artificial, sino en hacerlo sin validación, trazabilidad y supervisión humana. Estas exigencias deben organizar la gestión del riesgo de la información en varios niveles.

1. El primer nivel se relaciona con la alimentación del modelo. Para que una herramienta funcione de manera coherente en una investigación, requiere datos pertinentes. Su capacidad de responder al problema planteado depende de la información que el funcionario incorpora y de cómo la organiza. En consecuencia, debe existir una gestión rigurosa de los datos personales incluidos en el ámbito penal. Esto resulta especialmente delicado cuando se trata de información sobre salud, vida sexual, situación patrimonial, delitos o ejercicio de derechos personales reconocidos en la Constitución y en los tratados internacionales (Corte Constitucional del Ecuador, 2021, párr. 111).

El primer mecanismo de gestión del riesgo es, por ello, la captura lícita. Debe contar con una fuente lícita, con autorización judicial cuando corresponda, con medidas para minimizar las filtraciones y con una cadena de custodia. La incorporación de información a una herramienta no puede desligarse de las condiciones bajo las cuales fue obtenida. Si se pretende que el análisis contribuya al proceso penal, su origen y tratamiento deben poder ser explicados y controlados (Alibašić H.). Por lo tanto, la capacidad de correlacionar datos no subsana los problemas que puedan existir en su obtención.

A esto se añade una dificultad relativa a los entornos tecnológicos disponibles. Al menos en el foro público, no se identifica una oferta generalizada de módulos específicamente organizados para estos usos de seguridad, salvo mecanismos como

Palantir, que operan en entornos propios (Armstrong, 2026). Esto obliga a delimitar las herramientas utilizadas y a considerar software propietario cuya organización responda claramente a los actores involucrados. No basta con que una plataforma permita introducir información: debe existir claridad sobre el entorno en el que se procesa y sobre quiénes intervienen en su gestión.

2. El segundo nivel corresponde a la correlación. Corresponde preguntarse hasta qué punto los prompts y las solicitudes de recogida de información respetan los criterios técnicos, financieros, lingüísticos y victimológicos que orientan el análisis. En esta etapa aparece el riesgo de generar perfilamientos discriminatorios o escenarios que afecten derechos. La construcción de una solicitud no es una operación irrelevante: condiciona las relaciones que se buscan y las respuestas que se obtienen. Por eso, también debe examinarse cómo se formula la hipótesis y qué presupuestos se incorporan al pedir que la máquina relacione información.
3. El tercer nivel es la validación. Siempre debe existir lo que se conoce como *human in the loop*: una persona dentro del proceso que intervenga en la gestión y validación de los procedimientos (Slade, 2024). No se trata de añadir una presencia humana puramente formal, sino de contar con alguien capaz de contrastar los resultados. Este validador debe ser un miembro de las fuerzas y cuerpos de seguridad del Estado o de la Fiscalía cuya actuación tenga legitimidad y legalidad, y que pueda responder por lo que sucede con los datos.

La validación exige contraste pericial, explicación y revisión humana. El resultado producido por el sistema no debe aceptarse únicamente por su apariencia técnica o por la complejidad del procesamiento que lo precede. Tiene que existir una persona que comprenda su alcance y pueda explicar por qué resulta relevante para la investigación. La responsabilidad sobre la gestión de los procedimientos no puede desaparecer detrás de la herramienta. Precisamente porque el perfilamiento construye hipótesis, su validación debe mantener abierta la posibilidad de encontrar errores, inconsistencias o relaciones que no se sostengan.

Además, son necesarios mecanismos de control *ex post facto*. Lo producido debe trasladarse al proceso penal mediante actuaciones adecuadamente motivadas, dentro de las exigencias de seguridad jurídica del artículo 82 de la Constitución ecuatoriana. Debe garantizarse a la defensa el acceso a la información necesaria para examinar el perfilamiento y su transparencia algorítmica (Corte Constitucional de Colombia, 2025). La contradicción requiere que las partes puedan conocer cómo se obtuvo el resultado y no reciban solamente una conclusión



EL NUEVO
ECUADOR

Ministerio del Interior

presentada como técnicamente indiscutible. El control procesal debe alcanzar tanto la hipótesis como el procedimiento utilizado para construirla.

El juez también debe conocer cómo se generó el perfil: cuál fue la tecnología utilizada, qué datos se incorporaron y qué metodología orientó la construcción de los prompts. A ello deben sumarse medios de auditoría y reparación cuando exista un error. No es suficiente afirmar que hubo supervisión humana; es necesario que esa supervisión pueda ser examinada. La trazabilidad conecta la obtención de los datos, su procesamiento, la validación y la presentación procesal. Sin esa conexión, se dificulta determinar dónde surgió una equivocación y quién debía advertirla.

De este recorrido se desprenden tres conclusiones. La primera es que el perfilamiento criminal mediante inteligencia artificial es posible y puede ser útil porque acelera la gestión de información. Perfilar resulta valioso si reduce la incertidumbre y permite orientar mejor una investigación. Sin embargo, se vuelve peligroso cuando fabrica certezas no controladas, construidas sobre hipótesis falsas o violatorias de derechos. El criterio de valoración no debe ser únicamente la velocidad con la que se produce una respuesta, sino la posibilidad de someterla a verificación.

La segunda conclusión se refiere a la traducción de estas exigencias en protocolos de uso. Se requieren tres instrumentos: un protocolo transparente para las partes procesales, como ocurre con otros protocolos de Fiscalía; una bitácora de decisiones que permita reconstruir la transparencia algorítmica, conocer los prompts y comprender su manejo; y una auditoría de sesgos. Estos instrumentos deben hacer visible el recorrido de la información y las decisiones adoptadas durante su procesamiento. Su función es permitir que el uso de inteligencia artificial resulte comprensible y controlable dentro del proceso.

La auditoría de sesgos exige un trabajo interdisciplinario, inclusive jurídico y filosófico, acompañado de capacitación pericial. No se trata solamente de revisar si el sistema funciona técnicamente, sino de examinar cómo construye relaciones y qué consecuencias puede producir su utilización. La formación de quienes intervienen es parte de ese control: deben comprender tanto las posibilidades analíticas de la herramienta como sus límites. El trabajo interdisciplinario y la capacitación permiten sostener una revisión que no quede reducida a la confianza en el resultado automatizado.

Finalmente, ningún perfil sustituye la legalidad, la prueba, la contradicción ni la motivación judicial. Este es el límite que debe organizar toda la discusión. La inteligencia artificial puede ayudar a formular preguntas, conectar información y orientar hipótesis, pero su incorporación no transforma una correlación en una verdad procesal incontrovertible. Si el sistema es

acusatorio, corresponde conservar las condiciones que permiten discutir y probar lo que se afirma. El perfilamiento criminal digital tiene sentido dentro de esas condiciones: como instrumento de investigación sometido al Estado de Derecho, no como una vía para prescindir de él.

VÍCTIMAS, FACTORES DE VULNERABILIDAD Y SEÑALES DE ALERTA

Víctimas y sus perfiles

Las víctimas de estas conductas delictivas varían según la naturaleza de cada delito, aunque, de forma general, cualquier persona natural o jurídica puede verse afectada, sin importar su edad, género, nivel educativo o condición social. De acuerdo con las fuentes revisadas el mayor impacto se concentra en comerciantes, menores de edad, usuarios de servicios financieros y usuarios de redes sociales.

Los agresores buscan oportunidades y explotan las vulnerabilidades específicas en momentos determinados, por lo que la responsabilidad total del delito recae siempre en el agresor. (Interpol, s.f.)

A continuación, se detallan posibles perfiles de las víctimas y las conductas asociadas a cada delito:

Secuestro

Víctimas principales: Empresarios, comerciantes, transportistas, personas con alto poder adquisitivo y sus familiares directos. En modalidades como el "secuestro exprés", cualquier ciudadano que transite por zonas vulnerables puede ser el objetivo.

Conductas asociadas: Vigilancia y seguimiento de la rutina de la víctima, privación de la libertad, extorsión simultánea a familiares, lesiones físicas o psicológicas, y exigencia de rescates económicos.

Extorsión

Víctimas principales: Pequeños y medianos empresarios, comerciantes locales, trabajadores independientes, e incluso personas particulares a quienes les extraen información personal de sus perfiles digitales.

Conductas asociadas: Llamadas o mensajes intimidatorios, cobro de cuotas obligatorias (las llamadas "vacunas"), amenazas de atentar contra el negocio o la vida de la familia, empleo de violencia psicológica y exigencia de transferencias o retiros de dinero.



EL NUEVO
ECUADOR

Ministerio del Interior

Suplantación de identidad

Víctimas principales: Usuarios de la banca en línea, contribuyentes fiscales, profesionales con alta reputación y ciudadanos activos en redes sociales.

Conductas asociadas: Clonación de perfiles en redes sociales, robo de bases de datos, técnicas de engaño como el phishing (falsificación de correos institucionales o bancarios), apertura de créditos ilegales a nombre de terceros y falsificación de documentos de identidad. (Jumbo, 2025)

Ciberacoso

Víctimas principales: Niñas, niños, adolescentes y jóvenes, además de minorías o personas expuestas al escrutinio público en internet.

Conductas asociadas: Difusión de rumores falsos o contenido multimedia humillante, envío masivo de mensajes hostiles o amenazantes, doxing (exposición de datos privados o ubicaciones sin consentimiento), exclusión deliberada en plataformas digitales y la extorsión sexual. (MINTEL, s.f.)

Factores de vulnerabilidad

Ciertos elementos del entorno o de la situación de una persona pueden ser aprovechados por los delincuentes para facilitar sus ataques e incrementar su riesgo. Se agrupan en tres ámbitos:

Factores tecnológicos y de información

Publicar en redes sociales información personal, números de teléfono o correos electrónicos amplía la información que un desconocido puede averiguar. A ello se suma la exhibición de rutinas, al compartir los trayectos diarios, horarios fijos, lugares de estudio o centros de trabajo, y la geolocalización en tiempo real, al marcar la ubicación exacta de forma pública en fotografías o estados de plataformas digitales. Combinados, estos elementos permiten reconstruir los movimientos de una persona sin ningún contacto con ella.

Factores personales y relacionales

El riesgo también proviene del entorno cercano. Mantener o haber tenido una relación cercana, sentimental, laboral o familiar con el agresor facilita su acceso a información privada. A ese vínculo puede sumarse la dependencia emocional, es decir, la dificultad para cortar lazos con personas manipuladoras debido a dinámicas de control afectivo, o la dependencia económica, esto es, la subordinación financiera que limita la capacidad de alejarse de un entorno peligroso o violento.

Factores sociales y de vulnerabilidad

El aislamiento social, entendido como la ausencia de redes de apoyo familiares, de amigos o comunitarias que puedan intervenir o alertar, deja a la persona sin nadie que advierta el riesgo a tiempo. Esta condición se agrava en los grupos de atención prioritaria: niñas, niños, adolescentes, mujeres en situación de violencia, personas adultas mayores, personas con discapacidad o personas en situación de movilidad humana, que enfrentan barreras de protección históricas.

Estos tres ámbitos rara vez se presentan por separado. Cuando la exposición digital coincide con un vínculo previo o con la falta de apoyo cercano, el riesgo se multiplica y las afectaciones pueden afectar varios planos de la vida de la persona.

Impacto y afectaciones en las víctimas

Estas conductas delictivas provocan daños simultáneos en varios aspectos de la vida de quienes las padecen.

En el plano psicológico se presentan ansiedad severa, estrés persistente después de lo ocurrido, desconfianza constante, culpa injustificada, tristeza profunda e insomnio, que suelen prolongarse mucho después del hecho. En lo social, la ruptura de relaciones familiares, el aislamiento autoimpuesto por miedo, la estigmatización del entorno y el abandono escolar o laboral reducen la vida cotidiana de la persona afectada. A ello se añaden las consecuencias económicas: pérdida de ahorros por extorsión, gastos en mudanzas o seguridad, deudas adquiridas y pérdida de empleo; y las físicas, como los dolores crónicos por estrés, las alteraciones gastrointestinales o los daños derivados de agresiones físicas directas.

A todo lo anterior se suma el riesgo de un nuevo daño: la persona afectada vuelve a ser lastimada cuando su entorno la culpa, resta importancia a lo ocurrido, la obliga a repetir su relato una y otra vez o difunde su información privada.

Señales de alerta

La presencia de cualquiera de los siguientes indicadores requiere actuación inmediata. La respuesta temprana debe priorizar la seguridad, verificar la información por otros medios de contacto, conservar los mensajes, enlaces, cuentas y comprobantes, y comunicar el hecho de forma oportuna a las autoridades competentes, sin alterar ni difundir innecesariamente el contenido:

- Amenazas directas: Mensajes implícitos o explícitos de daño físico, difusión de material íntimo o destrucción de bienes.

- **Datos de geolocalización:** El agresor demuestra que conoce el domicilio, el lugar de trabajo, los centros de estudio o las actividades del entorno cercano.
- **Alusiones a terceros:** Mención de nombres, rutinas o ubicaciones de familiares, hijos o amigos para generar mayor presión.
- **Seguimiento físico:** Presencia de vehículos extraños, personas vigilando el entorno o encuentros "casuales" repetidos en la vía pública.
- **Acoso multicuenta:** Contacto con la víctima a través de múltiples perfiles falsos, diferentes números de teléfono o mediante intermediarios tras haber sido bloqueado.
- **Escalada de violencia:** Incremento notable en la frecuencia de los mensajes, el tono insultante, la exigencia del dinero o la gravedad de las advertencias, junto con la revelación de datos cada vez más precisos sobre la víctima.
- **Vulneración digital:** Accesos sin autorización a correos electrónicos, alertas de inicio de sesión en dispositivos desconocidos, cambios de contraseñas sin consentimiento o sospechas de software espía en el teléfono celular.

Ninguno de estos indicadores actúa de forma aislada pues su aparición combinada o su repetición en el tiempo señalan que el riesgo avanza. Reconocerlos a tiempo permite actuar antes de que la situación se agrave y facilita que las autoridades intervengan con información útil desde el primer momento.

PANORAMA ESTADÍSTICO

A continuación, se presentan casos relacionados con los delitos de secuestro, extorsión, suplantación de identidad y ciberacoso, con el propósito de contextualizar sus principales características, modalidades y la posible utilización de medios tecnológicos en su comisión. Posteriormente, se exponen las estadísticas de la Fiscalía General del Estado y del Consejo de la Judicatura, a fin de complementar el análisis de estos delitos en el país.

Casos documentados en el Ecuador

Los dos casos siguientes corresponden a hechos verificados y difundidos por fuentes oficiales. Muestran cómo las dinámicas descritas operan sobre personas concretas, en territorios y circunstancias reconocibles en la vida del ciudadano.



EL NUEVO
ECUADOR

Ministerio del Interior

Dos sentenciados como cómplices de secuestro extorsivo

En Riobamba, la Fiscalía General del Estado obtuvo una sentencia de 14 años, 2 meses y 15 días de prisión contra Julio Jefferson T. Q. y Jonathan Alberto V. L., como cómplices del delito de secuestro extorsivo. El secuestro ocurrió en agosto de 2025. (Fiscalía General del Estado, 2026)

Hechos del caso

Una mujer viajó desde el cantón Buena Fe hasta Riobamba para reunirse con la víctima. Después de ese encuentro, sus familiares y amigos perdieron contacto con él.

Horas después, la madre del afectado llamó al teléfono celular de su hijo; sin embargo, otra persona respondió la llamada y le informó que el vehículo en el que se movilizaba había sufrido un accidente de tránsito en la vía Pelileo-Baños.

Asimismo, le indicó que en el interior del automotor se encontraba el cuerpo sin vida de una mujer y que la víctima no se encontraba en el sitio del accidente.

Al siguiente día, el hermano del ciudadano recibió, a través de mensajes de WhatsApp, un video en el que este aparecía amarrado, con los ojos cubiertos y apuntado con un arma de fuego, mientras se encontraba en una zona selvática. Los secuestradores exigieron 250.000 dólares a cambio de su liberación.

Luego de permanecer más de veinticuatro días en cautiverio y tras varias negociaciones, el 2 de septiembre de 2025, el ciudadano fue liberado luego del pago de 6.000 dólares, monto que fue transferido a las cuentas bancarias de los sentenciados.

El medio digital Eco Amazónico sufrió una suplantación de identidad en Facebook

El medio digital Eco Amazónico alertó a sus lectores de que fue víctima de una suplantación de identidad. Con una etiqueta de “Falso”, el medio que cubre información de Pastaza aseveró que una cuenta “troll” está difundiendo posts y comunicados falsos, tomando su nombre, logotipo e imagen en Facebook.

Hechos del caso

El pasado 10 de abril, se publicó un comunicado que supuestamente pertenecía al asambleísta por Pastaza Faustino Fernández, en una página de Facebook con el nombre de ‘Eco Amazónico’. En dicho comunicado, se decía que Fernández aparentemente se solidarizaba con México, tras los hechos ocurridos en la Embajada de ese país en Ecuador. La página cuenta con el mismo logotipo, portada y nombre del medio digital; sin embargo, se trata de una página creada para difundir desinformación.

Tras viralizarse el falso comunicado, el medio desmintió categóricamente que la publicación sea de su autoría. Agregaron que se trataba de información falsa difundida por una cuenta impostora y reiteraron su compromiso de publicar únicamente contenido verificado. Además, hicieron un llamado a la ciudadanía a evitar la difusión de estos contenidos y a desconfiar de este tipo de engaños.

Estadísticas del fenómeno estudiado

Fiscalía General del Estado

Si bien algunos de estos delitos exceden la naturaleza estrictamente informática, actualmente pueden incorporar componentes digitales en diferentes etapas, como el contacto con las víctimas, la obtención de información personal, la intimidación, el engaño, el hostigamiento, la coordinación de acciones o la exigencia de beneficios económicos.

Tabla 2

Noticias del delito Fiscalía General del Estado

Noticias del delito					
Delito	2022	2023	2024	2025	2026 *
Secuestro	883	1640	1.939	1.794	658
Secuestro extorsivo	571	1.450	1.889	1.626	572
Extorsión	8.398	21.811	23.083	16.130	6.448
Extorsión sexual	80	155	164	187	107
Ciberacoso	86	110	94	70	48
Suplantación de Identidad	5.893	6.472	5.917	5.560	2.855
Total	15.911	31.638	33.086	25.367	10.688

Elaboración: Dirección de Ciberdelitos – Ministerio del Interior.

Fuente: Fiscalía General del Estado (* junio 2026)

Consejo de la Judicatura

El análisis del fenómeno de la ciberdelincuencia también comprende la respuesta del sistema de justicia frente a conductas delictivas que pueden incorporar el uso de tecnologías de la información y comunicación. En este sentido, los datos estadísticos analizados corresponden a las causas ingresadas y resueltas registradas por el Consejo de la Judicatura, relacionadas con los delitos de secuestro, extorsión, suplantación de identidad y ciberacoso.

Esta información permite conocer el comportamiento y evolución de los procesos judiciales asociados a estos delitos, así como establecer la relación entre las causas que ingresan al sistema de justicia y aquellas que han sido resueltas. Su análisis constituye un insumo para comprender la respuesta judicial frente a estas modalidades delictivas y contribuir al



fortalecimiento de las estrategias institucionales para la prevención y combate de la ciberdelincuencia.

Tabla 3

Causas ingresadas Consejo de la Judicatura

Causas ingresadas Consejo de la Judicatura					
Delito	2022	2023	2024	2025	2026 *
Secuestro	144	270	316	329	171
Secuestro extorsivo	159	387	637	822	388
Extorsión	238	454	984	1751	1453
Extorsión sexual	3	7	8	10	4
Ciberacoso	30	8	13	9	7
Suplantación de Identidad	191	178	159	145	74
Total	765	1.304	2.117	3.066	2.097

Elaboración: Dirección de Ciberdelitos - Ministerio del Interior.

Fuente: Consejo de la Judicatura (*junio 2026)

Tabla 4

Causas resueltas Consejo de la Judicatura

Causas Resueltas Consejo de la Judicatura					
Delito	2022	2023	2024	2025	2026
Secuestro	116	193	258	281	198
Secuestro extorsivo	103	251	434	627	372
Extorsión	198	338	668	1.208	1.121
Extorsión sexual	2	5	3	9	7
Ciberacoso	45	12	12	10	6
Suplantación de Identidad	179	187	140	175	74
Total	643	986	1.515	2.310	1.778

Elaboración: Dirección de Ciberdelitos - Ministerio del Interior.

Fuente: Consejo de la Judicatura (junio 2026)

MEDIDAS DE PREVENCIÓN Y RESPUESTA INSTITUCIONAL

El ordenamiento jurídico ecuatoriano protege a la ciudadanía frente a estos delitos en varios niveles, encabezados por el Artículo 66, numeral 19 de la Constitución de la República, que reconoce el derecho a la protección de datos de carácter personal, estructurados mediante la Ley Orgánica de Protección de Datos Personales (LOPD) y su Reglamento General.

En el ámbito penal, el Código Orgánico Integral Penal (COIP) tipifica y sanciona el secuestro extorsivo en su Artículo 162, la violación a la intimidad en el Artículo 178, la extorsión en el



Artículo 185, y los delitos contra la confidencialidad, disponibilidad e integridad de los datos y sistemas informáticos.

Recomendaciones multisectoriales de prevención y mitigación del riesgo

Las oportunidades de ataque se reducen de forma sustancial cuando cada sector adopta controles técnicos y normativos adaptados a su nivel de exposición.

Directrices de implementación por sector

Ciudadanía y núcleos familiares: Se recomienda limitar la exposición innecesaria de información personal en redes sociales y otros espacios digitales, especialmente aquella que permita identificar rutinas, ubicación, relaciones familiares, lugares de trabajo, centros educativos, números telefónicos u otros datos que puedan ser utilizados por la delincuencia para elaborar engaños, realizar suplantaciones o ejercer mecanismos de presión.

Como medida de protección de las cuentas digitales, se recomienda habilitar la autenticación de dos factores (2FA) en servicios de mensajería, correo electrónico, redes sociales y demás plataformas que dispongan de esta funcionalidad. Esta medida incorpora una verificación adicional a la contraseña y dificulta el acceso no autorizado a las cuentas.

En el ámbito familiar, resulta conveniente establecer mecanismos internos de verificación, como una palabra o código previamente acordado, que permita confirmar la identidad de un familiar ante llamadas o mensajes que informen sobre supuestas emergencias, accidentes, secuestros u otras situaciones utilizadas para generar presión o urgencia.

Ante este tipo de comunicaciones, se recomienda verificar la información directamente con la persona involucrada o mediante otro contacto de confianza antes de realizar transferencias económicas, proporcionar información personal o efectuar desplazamientos solicitados por el interlocutor.

Imagen 1

Recomendaciones Ciudadanía y Núcleos Familiares



Elaboración: Dirección de Ciberdelitos – Ministerio del Interior. Imagen generada con Gemini 3.6 Flash (2026), Google, <https://gemini.google.com>

Instituciones públicas y empresas privadas: Los responsables y encargados del tratamiento de datos deben dar estricto cumplimiento al Artículo 40 de la LOPDP mediante la ejecución periódica de análisis de riesgos, amenazas y vulnerabilidades, complementados con Evaluaciones de Impacto en la Protección de Datos Personales (EIPDP) según lo dispuesto en el Artículo 30 de la misma ley.

Asimismo, cuando la naturaleza o escala del tratamiento lo exija, las organizaciones deben designar un Delegado de Protección de Datos, responsable de vigilar el uso correcto de la información personal, formalizado en los términos del Artículo 50 del Reglamento General a la LOPDP.

Ante cualquier brecha de seguridad que comprometa la confidencialidad o integridad de la información sensible, las entidades tienen la obligación legal de notificar el incidente a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones (Arcotel) de acuerdo con los Artículos 24, 27 y 28 del citado Reglamento.



EL NUEVO
ECUADOR

Ministerio del Interior

Imagen 2

Recomendaciones Instituciones Públicas y Empresas Privadas



Elaboración: Dirección de Ciberdelitos – Ministerio del Interior. Imagen generada con Gemini 3.6 Flash (2026), Google, <https://gemini.google.com>

Centros educativos y grupos de atención prioritaria: En observancia del Artículo 44 de la Constitución de la República y las disposiciones garantistas del Código Orgánico de la Niñez y Adolescencia (CONA), las instituciones educativas asumen obligaciones específicas de protección frente a estas conductas.

Los directivos y docentes que identifiquen indicios de ciberacoso, grooming o extorsión dirigidos a niñas, niños o adolescentes están jurídicamente obligados a presentar la denuncia ante la autoridad competente en un plazo máximo de 48 horas, conforme al Artículo 13 del CONA.

Para los adultos mayores y personas con discapacidad, las entidades financieras y públicas deben adecuar canales asistidos de verificación para prevenir fraudes por ingeniería social y suplantación de identidad.



EL NUEVO
ECUADOR

Ministerio del Interior

Imagen 3

Recomendaciones Centros Educativos y Grupos de Atención Prioritaria



Elaboración: Dirección de Ciberdelitos – Ministerio del Interior. Imagen generada con Gemini 3.6 Flash (2026), Google, <https://gemini.google.com>

Tabla 5

Matriz de Controles Preventivos Multisectoriales

Matriz de controles preventivos por sectores		
Sector objetivo	Riesgo principal asociado	Medida preventiva / Acción directa
Ciudadanía y familias	Extorsión, secuestro extorsivo y ciberacoso derivado de la exposición involuntaria de datos personales y de la ubicación en tiempo real.	Restringir la privacidad en redes sociales, desactivar la geolocalización en tiempo real de los dispositivos y validar la identidad de interlocutores desconocidos antes de proporcionar información sensible o financiera.
Instituciones públicas	Suplantación de identidad institucional, fuga de bases de datos de ciudadanos y robo de contraseñas mediante engaño (<i>phishing</i>) al personal administrativo.	Implementar controles de protección de datos conforme a la normativa vigente, reforzar la seguridad de los servidores, aplicar de forma obligatoria la verificación en dos pasos y ejecutar auditorías técnicas periódicas.



EL NUEVO
ECUADOR

Ministerio del Interior

Empresas privadas	Extorsión digital mediante secuestro de datos (<i>ransomware</i>), fraude por suplantación de directivos y compromiso de activos críticos.	Desarrollar planes de continuidad de negocio, cifrar bases de datos transaccionales, implementar protocolos estrictos de verificación de pagos y capacitar continuamente al personal en ingeniería social.
Centros educativos	Ciberacoso escolar, contacto engañoso de adultos con menores con fines sexuales (grooming), suplantación de identidad de estudiantes o docentes y difusión de imágenes sin consentimiento.	Establecer protocolos institucionales de convivencia digital, segmentar las redes Wi-Fi institucionales, impartir talleres de alfabetización digital segura y habilitar canales confidenciales para la recepción de alertas.
Grupos de atención prioritaria	Ingeniería social coercitiva, estafas telefónicas dirigidas a adultos mayores y violencia digital contra niños, niñas, adolescentes y personas con discapacidad.	Implementar programas adaptados de ciberseguridad comunitaria, promover la supervisión parental proactiva mediante herramientas de control de contenidos y establecer redes de acompañamiento familiar directo para la gestión de trámites.

Elaboración: Dirección de Ciberdelitos – Ministerio del Interior.

Ejes técnicos y operativos

Verificación de identidad y reducción de huella digital

Las organizaciones y los ciudadanos deben aplicar de manera sistemática el principio de publicar la menor cantidad posible de datos, revisando periódicamente la información institucional o personal expuesta en motores de búsqueda, registros públicos digitales y plataformas de redes sociales (National Institute of Standards and Technology [NIST], 2020).

Para dificultar el perfilamiento que precede a la extorsión o a la suplantación de identidad, resulta imprescindible eliminar los datos que el propio archivo almacena (metadatos) antes de publicar una fotografía o un video. Esta práctica impide que la delincuencia obtenga el lugar, la fecha y la hora en que se tomó la imagen, así como el dispositivo utilizado (Centro de Respuestas a Incidentes Informáticos [ECU-CERT], 2023). Cortar de raíz esa recolección de información elimina el insumo principal que sustenta las amenazas tipificadas en el artículo 185 del Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014), reduciendo la probabilidad de que una persona o entidad sea seleccionada como blanco de extorsión.



EL NUEVO
ECUADOR

Ministerio del Interior

Fortalecimiento de cuentas y preservación de evidencia digital

Para reforzar la verificación en dos pasos conviene utilizar una aplicación de autenticación o una llave de seguridad física, en lugar de los códigos enviados por mensaje de texto, expuestos a la duplicación fraudulenta de la tarjeta SIM (International Organization for Standardization [ISO], 2022). De igual manera, el uso de aplicaciones de mensajería que cifran las conversaciones de extremo a extremo y de un gestor de contraseñas reduce de forma significativa el riesgo de suplantación de identidad.

Cuando la infracción se consuma, la preservación de la evidencia digital resulta determinante para sostener su validez durante el proceso. De acuerdo con el artículo 500 del Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014), el personal especializado aplica procedimientos que acreditan la integridad de cada elemento y mantienen intacta la cadena de custodia durante la investigación. Para la ciudadanía la regla práctica es sencilla: conservar los mensajes, las capturas y los dispositivos tal como están y entregarlos a la autoridad sin modificarlos.

Gestión de amenazas y protección de víctimas

La respuesta inmediata ante incidentes extorsivos o de ciberacoso requiere una evaluación de riesgos estandarizada que valore en tiempo real qué tan creíble y peligrosa resulta la amenaza. Esa valoración determina si se trata de un engaño masivo enviado al azar o de una amenaza dirigida contra una persona concreta, acompañada de vigilancia sobre el terreno, activando los protocolos diferenciados de protección física y digital (Ministerio del Interior del Ecuador, 2023). En los casos que involucran violencia digital contra sectores vulnerables o mujeres, las medidas de gestión del riesgo se coordinan con las salvaguardas establecidas en la Ley Orgánica para Prevenir y Erradicar la Violencia contra las Mujeres (Asamblea Nacional del Ecuador, 2018), garantizando el cese inmediato de la interacción violenta y la aplicación de medidas de protección urgentes.

Mecanismos de articulación interinstitucional

La respuesta del Estado ecuatoriano frente a los delitos cibernéticos y de alto impacto se articula mediante un flujo de trabajo interinstitucional integrado. Ante una alerta receptada por el Servicio Integrado de Seguridad ECU 911, los protocolos disponen la derivación inmediata del caso a la Policía Nacional del Ecuador y a sus unidades especializadas: la Unidad Anti-Secuestros y Extorsión (UNASE), la Dirección Nacional de Investigación de Delitos Contra la Vida (DINASED) y el Bloque de Ciberdelitos de la Policía Judicial (Fiscalía General del Estado, 2023). La actuación se coordina con la Fiscalía General del Estado (FGE) para la apertura del acto

urgente o la investigación previa, garantizando que las diligencias investigativas cuenten con el debido control jurisdiccional del Consejo de la Judicatura (Ministerio del Interior del Ecuador, 2023).

Adicionalmente, la eficacia del combate al ciberdelito depende de las alianzas operativas con el sector privado y las plataformas tecnológicas internacionales. Los mecanismos de cooperación técnica vigentes facilitan tramitaciones expeditas para el requerimiento de preservación de datos y revelación de registros ante proveedores de servicios de internet (ISP) y plataformas transnacionales bajo tratados de asistencia legal mutua (Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL], 2022). Esta sinergia pública-privada, complementada por la academia y los equipos de respuesta a incidentes de seguridad informática (CSIRTs), robustece el ecosistema nacional de ciberdefensa y acelera la persecución penal de las organizaciones delictivas.

Acciones cuando existe riesgo para la vida

- **Resguardo inmediato de la víctima:** Reubicar de inmediato a la persona amenazada en un espacio seguro y neutral, fuera de la ruta habitual o del alcance visual y digital directo de los presuntos agresores.
- **Suspensión de la confrontación y negociación informal:** Abstenerse de confrontar, insultar o negociar de manera autónoma con los extorsionadores. Evitar los pagos y las promesas de entrega de dinero o bienes, ya que esto perpetúa la coerción y aumenta la vulnerabilidad.
- **Fijación técnica y conservación de la evidencia digital:** Conservar íntegros los chats, audios, correos electrónicos e historiales de llamadas. Tomar capturas de pantalla donde se observe claramente el contenido de los mensajes, las fechas, las horas, las direcciones URL y los números de teléfono emisores.
- **Activación de canales oficiales de emergencia:** Marcar inmediatamente al ECU 911 o a la línea confidencial 1800-DELITO (1800-335486) para solicitar la intervención directa y el acompañamiento especializado de la UNASE y la DINASED de la Policía Nacional.



EL NUEVO
ECUADOR

Ministerio del Interior

CONCLUSIONES

- El análisis de la ciberdelincuencia desarrollado en este boletín evidencia que la delincuencia en el Ecuador ha evolucionado hacia un modelo operativo dinámico, donde las tecnologías emergentes, la inteligencia artificial y los entornos virtuales facilitan delitos como la extorsión, la suplantación de identidad, el secuestro y el ciberacoso, y actúan además como herramientas de inteligencia táctica para la logística y preparación de los delitos. Frente a esta realidad, las respuestas tradicionales del Estado resultan insuficientes si no se respaldan en un enfoque multidisciplinario, preventivo y sustentado en el rigor forense.
- En este contexto, la investigación reafirma la necesidad de una articulación interinstitucional ágil y efectiva entre el ECU 911, la Policía Nacional a través de sus unidades especializadas, la Fiscalía General del Estado y los proveedores de tecnología, con el propósito de preservar la evidencia digital y fortalecer la capacidad de respuesta frente al ciberdelito.
- Se evidencia la importancia de estandarizar los canales de denuncia, consolidar los sistemas estadísticos y operativos, y promover la prevención del ciberdelito mediante la concientización ciudadana. Este esfuerzo debe orientarse hacia la adopción de mecanismos de ciberseguridad en el uso cotidiano de redes sociales y del internet en general, garantizando así una cultura digital responsable y resiliente. Las cifras muestran una brecha entre las denuncias y las causas judicializadas, especialmente en extorsión, extorsión sexual y suplantación de identidad. Reducirla exige mejorar la calidad de los registros, la preservación temprana de la evidencia digital y el análisis de patrones que permita relacionar hechos aparentemente aislados, siempre bajo validación humana y control jurídico.
- La acción más eficaz al alcance de la ciudadanía consiste en resguardar la información que documenta el hecho y acudir de inmediato a los canales oficiales. Conservar íntegros los mensajes, capturas, enlaces y comprobantes, evitar cualquier pago a quien amenaza y denunciar ante el ECU 911 o la línea 1800-DELITO (1800-335486) permite que la investigación avance y que un hecho aparentemente aislado se relacione con otros ya registrados.



GLOSARIO DE TÉRMINOS

Ciberdelincuencia. Conjunto de delitos que se cometen a través de internet, dispositivos o redes digitales, sea porque atacan directamente esos medios o porque los emplean para ejecutar conductas ya previstas en la ley (Interpol, s.f.).

Doxing. Difusión pública de datos privados de una persona, como su domicilio, lugar de trabajo, número telefónico o ubicación, sin su consentimiento, para exponerla, intimidarla o facilitar que terceros la agredan (MINTEL, s.f.).

Evidencia digital. Mensajes, capturas de pantalla, audios, videos, registros de llamadas y comprobantes que respaldan un hecho denunciado. Conserva su valor ante la autoridad cuando se la mantiene íntegra y sin modificaciones, conforme al artículo 500 del Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014).

Extorsión sexual. Conducta mediante la cual, con violencia, amenazas o chantaje, se obliga a una persona a exhibir su cuerpo o a realizar actos de carácter sexual para obtener un provecho. Se encuentra tipificada en el artículo 172.1 del Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014).

Grooming. Acercamiento engañoso de una persona adulta a una niña, niño o adolescente por medios digitales, con la finalidad de ganar su confianza y obtener contenido o encuentros de carácter sexual (MINTEL, s.f.).

Ingeniería social. Técnicas de engaño dirigidas a que una persona entregue información, dinero o acceso a sus cuentas por voluntad propia, mediante la manipulación de su confianza, su urgencia o su temor (Europol, 2024).

Modus operandi. Forma habitual de actuar que se repite entre distintos hechos: el canal de contacto, el tipo de mensaje, los plazos exigidos y las acciones posteriores. Su análisis permite plantear hipótesis sobre la posible relación entre casos (Burrell et al., 2024).

Phishing. Mensaje que imita la comunicación de un banco, una institución o una empresa conocida para que la persona entregue sus contraseñas o datos bancarios. Llegaba habitualmente por correo electrónico, mensaje de texto o redes sociales (Centro de Respuestas a Incidentes Informáticos [ECU-CERT], 2023).

Ransomware. Programa que bloquea los archivos de un equipo o de una organización y exige un pago para devolver el acceso. Se lo conoce también como secuestro de datos (Centro de Respuestas a Incidentes Informáticos [ECU-CERT], 2023).

Suplantación de identidad. Uso de la identidad de otra persona para obtener un beneficio propio o de un tercero, en perjuicio de la persona suplantada. Se encuentra tipificada en



EL NUEVO
ECUADOR

Ministerio del Interior

el artículo 212 del Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014).

Verificación en dos pasos. Medida de seguridad que añade un segundo requisito al iniciar sesión, además de la contraseña: un código temporal generado por una aplicación o una llave de seguridad física. Protege la cuenta aun cuando la contraseña quede expuesta (National Institute of Standards and Technology [NIST], 2020).



EL NUEVO
ECUADOR

Ministerio del Interior

BIBLIOGRAFÍA

Alibašić, H. (2026). Untangling the Algorithmic Leviathan: Palantir, the Post-Factual Polity, and the Infrastructural Crisis of AI Governance in Public Administration. *Systems*, 14(7), 879. <https://doi.org/10.3390/systems14070879>.

Anthropic. (2026). Detecting and countering misuse of AI: September 2026. <https://www.anthropic.com/threat-intelligence-report-september-2026>.

Armstrong, S. (2026). Palantir: NHS England admits data don't prove contentious software benefits health service. *BMJ*, 393, e100110. <https://doi.org/10.1136/bmj-2026-100110>

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal [COIP]. Registro Oficial Suplemento 180 de 10 de febrero de 2014.

Asamblea Nacional del Ecuador. (2018). Ley Orgánica para Prevenir y Erradicar la Violencia contra las Mujeres. Registro Oficial Suplemento 175 de 05 de febrero de 2018.

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales [LOPDP]. Registro Oficial Suplemento 459 de 26 de mayo de 2021.

Burrell, A., Costello, B., & Woodhams, J. (2024). Methods used to link crimes using behaviour: A literature review. *Aggression and Violent Behavior*, 76, 102014.

Centro de Respuestas a Incidentes Informáticos. (2023). Guía de buenas prácticas de ciberseguridad y protección de datos personales en el entorno digital. Ministerio de Telecomunicaciones y de la Sociedad de la Información.

Corte Constitucional de Colombia. (2025, 26 de febrero). Sentencia T-067/25 (Expediente T-8.202.533; N. Ángel Cabo, M. P.). <https://www.corteconstitucional.gov.co/relatoria/2025/t-067-25.htm>

Corte Constitucional del Ecuador. (2021, 27 de enero). Sentencia n.º 2064-14-EP/21.

Corte Constitucional del Ecuador. (2022, 27 de enero). Sentencia n.º 77-16-IN/22.

Europol. (2024). Internet organised crime threat assessment (IOCTA) 2024. Publications Office of the European Union.

Federal Bureau of Investigation. (2025, 5 de diciembre). Criminals using altered proof-of-life media to extort victims in virtual kidnapping for ransom scams (Alerta I-120525-PSA). Internet Crime Complaint Center. <https://www.ic3.gov/PSA/2025/PSA251205>



EL NUEVO
ECUADOR

Ministerio del Interior

Fiscalía General del Estado. (08 de 09 de 2026). Boletines de prensa FGE. Recuperado el 09 de 09 de 2026, de <https://www.fiscalia.gob.ec/2-sentenciados-como-complices-de-secuestro-extorsivo/>

Fiscalía General del Estado. (2023). Informe de gestión y protocolos de investigación en delitos de ciberdelincuencia, extorsión y secuestro. FGE Ecuador.

International Organization for Standardization. (2012). Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC Standard No. 27037:2012). <https://www.iso.org/standard/44381.html>

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security controls (ISO/IEC Standard No. 27001:2022). <https://www.iso.org/standard/82875.html>

Interpol. (s.f.). La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad. Recuperado el 04 de 09 de 2026, de <https://www.interpol.int/es/Delitos/Ciberdelincuencia>

Jumbo, C. (2025). La Suplantación de Identidad Digital en el COIP: Análisis Jurídico de las Dificultades de Aplicación y su Impacto en el Derecho a la Tutela Judicial Efectiva de las Víctimas en Ecuador. *Polo del Conocimiento*, 10(10). doi:<https://doi.org/10.23857/pc.v10i10.10539>

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking: An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, 163, 120426.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-86>

Martineau, M., Spiridon, E., & Aiken, M. (2023). A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature. *Forensic Sciences*, 3(3), 452–477. <https://doi.org/10.3390/forensicsci3030032>

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). Estrategia Nacional de Ciberseguridad del Ecuador. MINTEL.

Ministerio del Interior del Ecuador. (2023). Protocolo de actuación interinstitucional contra la extorsión y la violencia cibernética. Gobierno de la República del Ecuador.



EL NUEVO
ECUADOR

Ministerio del Interior

MINTEL. (s.f.). <https://www.telecomunicaciones.gob.ec/conoce-mas-ciberacoso/>. Recuperado el 04 de 09 de 2026, de <https://www.telecomunicaciones.gob.ec/conoce-mas-ciberacoso/>

National Institute of Standards and Technology. (2020). Digital identity guidelines (NIST Special Publication 800-63-3). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-63-3>

Oficina de las Naciones Unidas contra la Droga y el Delito. (2022). Compendio de ciberdelincuencia organizada. Naciones Unidas.

Policía Nacional del Ecuador. (2022). Manual de procedimiento operativo para la atención de casos de secuestro y extorsión. Dirección Nacional de Investigación Criminal.

Slade, P., Atkeson, C., Donelan, J. M., Houdijk, H., Ingraham, K. A., Kim, M., ... & Collins, S. H. (2024). On human-in-the-loop optimization of human–robot interaction. *Nature*, 633(8031), 779–788.

Starace, J. (2026). Which truths to tell: Misdirection, belief opacity, and adversarial manipulation of profiled LLM agents [Tesis doctoral, University of Idaho].

Subrahmanyam, S. (2026). Preparing for the next generation of AI impacts on belief systems. En S. Chakraborty (Ed.), *Intersections of AI and the freedom of religion or belief* (pp. 49–80). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3373-3830-9.ch003>

Subramaniam, K. N. S. (2026). Regulating AI in criminal justice: A study on surveillance technologies, predicative policing, cybercrime enforcement, and human rights protection. En V. S. Yadav & A. B. Puthupurakizhakathil (Eds.), *Proceedings of the International Conference on Socio-Legal Intricacies of Artificial Intelligence (ICSLIAI 2026)* (pp. 146–152). Atlantis Press. https://doi.org/10.2991/978-2-38476-547-8_18.

Véliz, C. (2026). Profecía: Lecciones sobre el uso y abuso de la predicción, desde los antiguos oráculos hasta la IA (Á. Marcos Lantero & A. Barba, Trans.). Debate.



EL NUEVO
ECUADOR

Ministerio del Interior