ANÁLISIS DE LA CIBEDELINCUENCIA

BOLETÍN

EN ESTA EDICIÓN

LA CIBERDELINCUENCIA COMO SERVICIO

Copyright @2025

DIRECCIÓN DE CIBERDELITOS
MINISTERIO DEL INTERIOR

Boletín de Análisis: “La ciberdelincuencia como Servicio”
Ministerio del Interior
Subsecretaría de Combate al Delito
Dirección de Ciberdelitos

Presidente de la República
MAGISTER DANIEL ROY-GILCHRIST NOBOA AZÍN

Ministro del Interior
Sr. JOHN REIMBERG OVIEDO

Subsecretario de Combate al Delito
TENIENTE CORONEL (SP) LUIS FERNANDO PÉREZ DÁVILA

Director de Ciberdelitos
MAGISTER JORGE FERNANDO ILLESCAS PEÑA

Responsables y Colaboradores

Redacción técnica del documento:
INGENIERO DIEGO TEJADA CAMPOS, Analista de Ciberdelitos
MAGISTER MARIO SIGCHA MOROCHZ., Analista de Ciberdelitos
MAGISTER GABRIEL REINOSO MARTÍNEZ, Analista de Ciberdelitos
MAGISTER CARLOS SIMBAÑA COBA, Analista de Ciberdelitos
INGENIERO CÉSAR TRELLES SEGOVIA, Analista de Ciberdelitos
INGENIERO WILLIAM IBARRA FLORES, Analista de Ciberdelitos

Revisión técnica del documento:
MAGISTER JORGE NÉJER GUERRERO, Especialista de Ciberdelitos
MAGISTER FERNANDO MOYA LEIMBERG, Especialista de Ciberdelitos
INGENIERO FREDDY GALLARDO SOSA, Especialista de Ciberdelitos

Redacción y compilación:
MAGISTER DUVAL MONTATIXE CAIZALUISA, Analista de Ciberdelitos

Edición y Adaptación:
MAGISTER DUVAL MONTATIXE CAIZALUISA, Analista de Ciberdelitos

@Mayo 2025

EL NUEVO ECUADOR
Ministerio del Interior

Tabla de contenido

Contenido

PRESENTACIÓN

La era digital ha transformado el panorama delictivo, facilitando que la delincuencia opere con mayor efectividad, se consolide como una industria multimillonaria, con ataques dirigidos a empresas, gobiernos y usuarios. En Ecuador, los delitos informáticos han experimentado un crecimiento exponencial, afectando a múltiples sectores tanto gubernamentales como privados.

La Ciberdelincuencia como Servicio (CaaS) es un modelo donde herramientas y servicios ilícitos se comercializan, permitiendo que cualquier organización criminal o persona, pueda llevar a cabo prácticas ilícitas a cambio de un pago o por alguna motivación específica, convirtiendo este fenómeno en una amenaza creciente que democratiza el ciberdelito, haciéndolo accesible a individuos y organizaciones independientemente de sus habilidades técnicas. El anonimato de la web oscura y el uso de medios de pago digitales, han convertido a la ciberdelincuencia en una actividad altamente rentable para los atacantes.

La Ciberdelincuencia como Servicio (CaaS) representa un desafío creciente para la seguridad digital. Se necesita una respuesta integral que combine tecnología, educación y políticas de combate a la ciberdelincuencia para enfrentar esta amenaza en constante evolución.

Dirección de Ciberdelitos del Ministerio del Interior

INTRODUCCIÓN

La Ciberdelincuencia como Servicio (CaaS) ha surgido como una nueva modalidad en la que operan grupos de delincuencia organizada, activistas, ciberdelincuentes tradicionales, entre otros, aprovechando las tecnologías de la información y comunicación (TIC) para cometer el delito. Este modelo permite contratar servicios especializados, sin necesidad de poseer conocimientos técnicos avanzados, permitiéndoles mimetizarse y actuar de manera más efectiva. Entre estos se incluyen ataques de ransomware, robo de datos personales, criptominería no autorizada, phishing especializado, entre otros.

La CaaS ha generado un gran mercado digital, donde se comercializan herramientas como botnets, exploits, ataques DDoS y malware personalizado, disponibles en foros clandestinos en la deep web y dark web. Además, ha facilitado la colaboración entre ciberdelincuentes, creando redes criminales más sofisticadas.

El boletín "La Ciberdelincuencia como Servicio" servirá como guía de referencia para profesionales, investigadores policiales y funcionarios de justicia penal, ayudando a reconocer y comprender estos delitos cometidos mediante el uso de las TIC, así como a mejorar la investigación relacionada con la ciberdelincuencia organizada y las nuevas modalidades de ciberdelito.

CONTEXTUALIZANDO LA CIBERDELENCUENCIA COMO SERVICIO (CAAS)

Desde los inicios de los sistemas y redes telefónicas, han existido individuos que han buscado formas de manipularlos en su beneficio, incluso si solo era para obtener llamadas de larga distancia gratuitas.

A medida que la tecnología avanzaba y se integraba en diferentes aspectos de la vida cotidiana, las oportunidades para la manipulación de sistemas se expandieron más allá de las telecomunicaciones (Allodi, 2015).

A finales de la década de los noventa, se introdujo el término *"ciberdelito"* para referirse a los delitos cometidos a través del uso de las TIC's. (Unir, 2021)

En el ordenamiento jurídico ecuatoriano, la ciberdelincuencia bajo el modelo *Crime-as-a-Service* encuentra su abordaje legal principalmente en los artículos 231 al 234.4 del Código Orgánico Integral Penal (COIP), donde se tipifican conductas como la Interceptación ilegal de datos, la Ataque a la integridad de sistemas informáticos, Acceso no consentido a un sistema informático, telemático o de telecomunicaciones, Falsificación informática. Estas disposiciones sancionan con penas privativas de libertad de tres a siete años, agravándose si los ataques afectan servicios públicos, infraestructuras críticas o sistemas vinculados a la seguridad ciudadana.

Este marco legal permite perseguir penalmente tanto a quienes desarrollan y comercializan herramientas maliciosas, como a quienes las adquieren y utilizan con fines delictivos, reproduciendo el esquema de servicios "*a la carta*" propio del modelo CaaS. Además, el artículo 234.3 establece la responsabilidad penal de las personas jurídicas, permitiendo sancionar a entidades que participen o faciliten la comisión de estos delitos. Así, Ecuador no solo reconoce este fenómeno emergente, sino que lo enfrenta mediante herramientas normativas que buscan mitigar su proliferación en el entorno digital.

La aparición del modelo "como servicio" en TI (software como servicio, plataformas como servicio, entre otros); también ha sido adoptado por la ciberdelincuencia transformándola en

una actividad lucrativa y accesible, donde ciberdelincuentes ofrecen herramientas, servicios y asistencia técnica a otros delincuentes, a cambio de un pago. Al igual que en los servicios en la nube legítimos, los atacantes pueden alquilar o comprar herramientas para llevar a cabo sus ataques sin necesidad de poseer habilidades avanzadas en hacking. (Zuluaga, 2025)

El crecimiento de la CaaS ha sido impulsado por varios factores interrelacionados que han facilitado su proliferación a nivel mundial aprovechando el entorno digital, como el anonimato proporcionado por la dark web, el uso de criptomonedas que dificulta a las fuerzas de seguridad el rastreo de pagos y localización de los ciberdelincuentes les, creando un entorno propicio para las actividades ilegales.

Entre algunos de los servicios que se ofrecen bajo el modelo CaaS tenemos los siguientes:

RaaS: hace referencia al Ransomware como servicio en donde personas pueden obtener paquetes de software malicioso que cifra los datos de la víctima y exige un rescate para su liberación. (Alto, 2025)

Phishing como servicio (**PhaaS):** Se caracteriza porque sus kits están orientados a aprovechar la ingeniería social, manipulando la confianza de las víctimas para robar fondos o datos confidenciales. (Pujara, 2018)

Malware as a service (**MaaS):** El malware como servicio es un ciberdelito en el que los delincuentes crean software y hardware maliciosos y los venden o alquilan a otros hackers en la red oscura. (Rudra, 2025)

Ataque de denegación de servicio distribuido (DDoS): servicio que permiten a los usuarios interrumpir los servicios de la víctima al saturar una red con tráfico. (Cloudflare, 2025)

Las actividades delictivas en el entorno digital han dado lugar a un mercado clandestino donde se comercializan diversos servicios utilizados para llevar a cabo ataques cibernéticos. En este contexto, la Tabla 1 presenta los servicios más empleados por los ciberdelincuentes y los principales objetivos a los que van dirigidos, según el análisis de Joshua Cena (Cena & Liang, 2023)

***Tabla 1**: Servicios de ciberdelincuencia, costos y objetivos comunes*

Servicio	Porcentaje de uso	Costo promedio (USD)	Objetivo
Ransomware	45%	$300-1500	Corporaciones, Individuos
DDoS	25%	$20-150	Websites, comercio electrónico
Phishing	20%	$10-200	Instituciones financieras
Malware	10%	$100-500	Gobierno, atención médica

***Fuente:** El ciberdelito como servicio: una amenaza creciente* (Cena & Liang, 2023)

La tabla 2 hace referencia a las pérdidas financieras en la industria que fueron provocadas por servicios relacionados con CaaS según Joshua Cena. (Cena & Liang, 2023)

***Tabla 2**: Pérdidas financieras relacionadas con CaaS en las industrias*

Industria	Costo promedio del ataque (USD)	Frecuencia del ataque	Ataques comunes via CaaS
Salud	$7.1 M	Alta	Ransomware, Phishing
Servicios financieros	$5.9 M	Alta	Ransomware, DDoS
Energía y servicio público	$4.7 M	Moderada	Malware, DDoS
Retail y comercio electrónico	$ 3.4 M	Alta	Phishing
Gobierno	$6.5 M	Moderada	Malware

***Fuente:** El ciberdelito como servicio: una amenaza creciente* (Cena & Liang, 2023)

Según las proyecciones de '*Cybercrime Magazine'*, se prevé que el coste global de los ciberdelitos a nivel mundial alcance los 10,5 billones de dólares en 2025. (Freeze, 2018)

Dada la creciente amenaza que plantea CaaS, las organizaciones deben adoptar un enfoque multifacético para protegerse contra estos ataques. Algunas estrategias de mitigación clave deberían incluir:

- **Medidas de ciberseguridad mejoradas**: Implementar sistemas de cifrado fuertes, firewalls y sistemas de detección de intrusos con IA
- **Capacitación de empleados**: Planes de capacitación regulares para aumentar la conciencia sobre los ataques de phishing y las amenazas de malware, manteniendo al personal actualizado y alerta.
- **Planes de respuesta a incidentes**: Desarrollar protocolos de respuesta a incidentes sólidos y articulados entre dependencias o instituciones para minimizar el daño en caso de una infracción.
- **Colaboración con las fuerzas del orden**: Fortalecer la cooperación internacional para rastrear pagos sospechosos o contenido ilegal y planes legales articulados para detener a los cibercriminales.

El auge del modelo del Ciberdelito como Servicio (CaaS) evidencia una alarmante evolución, donde la facilidad de acceso, el anonimato y la alta rentabilidad han generado un ecosistema criminal sofisticado y accesible. Este fenómeno ha provocado impactos significativos en múltiples sectores, afectando desde la infraestructura crítica hasta la vida cotidiana de ciudadanos y empresas. Frente a este desafío creciente, es dispensable una respuesta integral que combine tecnología, concientización y cooperación.

Si bien el marco legal ecuatoriano, a través del COIP, ha dado pasos importantes al tipificar y sancionar diversas conductas delictivas asociadas al CaaS, persisten desafíos significativos en la educación, concienciación y preparación de la población, así como en la necesidad de fortalecer y actualizar la normativa para enfrentar la sofisticación y el alcance de estos delitos digitales.

PANORAMA GEO CIBERDELINCUENCIAL

Enfoque Mundial

A continuación, se presentan casos de incidentes realizados a nivel mundial, que evidencian la magnitud y el alcance de esta amenaza.

Ransomware como servicio (RaaS)

En 2023, el ransomware BlackCat (ALPHV) atacó a Henry Schein, una empresa de asistencia sanitaria, robando 35 TB de datos. (Gatlan, S., 2024)

Malware como servicio(MaaS)

En 2024, Grandoreiro conocido troyano bancario de origen brasileño, ha atacado a más de 1700 bancos y criptocarteras en 45 países. En España, ha causado fraudes por al menos 3.5 millones de euros. (kaspersky, 2024)

Phishing como servicio (PhaaS)

En 2024 la plataforma de phishing como servicio LabHost ofrece suscripciones desde $179 hasta $300 al mes para atacar bancos y servicios digitales. (Trend Micro, 2024)

Microsoft confiscó 240 dominios usados por la plataforma ONNX para ataques contra empresas como Google y Dropbox. (Gatlan, S., 2024)

Fraude como servicio (FaaS)

Según la Encuesta de Fraude de Ravelin para 2023, el 56% de los analistas de fraude en todo el mundo han visto planes de fraude como servicio contra sus empresas. Canadá y Australia lideran la lista, con el 67% y 66% respectivamente, los encuestados señalaron a FaaS como un tipo de fraude con el que se han visto afectados. (Omo-Ikerodah, 2024)

Enfoque Regional

El panorama del CaaS en América Latina para 2025 se presenta como un desafío creciente, impulsado por la expansión del acceso a internet y la digitalización de diversos sectores. Los ciberincidentes en América Latina han aumentado un 25% anual durante la última década. (Bocconi, 2025)

Según Kaspersky (2024), entre junio de 2023 y julio de 2024, la región sufrió más de 1,1 billones de ataques de malware, con un promedio de 3,1 millones de incidentes diarios. Las principales amenazas incluyen adware, troyanos y herramientas de acceso remoto. Países como República Dominicana, Uruguay y Argentina han registrado los mayores aumentos en ataques, lo que subraya la necesidad de fortalecer la ciberseguridad mediante educación digital, protección de sistemas críticos y cooperación regional. (Kaspersky, 2024)

Enfoque Local

Los delitos cometidos con el uso de las TIC han aumentado en Ecuador y América Latina en la última década. Se estima que el 80% de estos delitos no se reportan y Ecuador ocupa el tercer lugar en la región, después de México y Bolivia. (Ponce M., Delitos informáticos: Caso Ecuador, 2024)

Esto evidencia la importancia de fortalecer la cultura de prevención y denuncia, para lo cual el Ministerio del Interior, a través de la Dirección de Ciberdelitos, elabora guías orientadas a la ciudadanía como parte de su estrategia de acción.

Pese a los esfuerzos, el país ha sido blanco de ciberataques de gran impacto, como el ransomware BlackCat en el Municipio de Quito en abril de 2024, que comprometió el 20% de su base de datos). (Technologies, 2025)

Para hacer frente a estas amenazas, el Ecuador ha participado en operaciones internacionales para combatir redes de ciberdelincuencia. En septiembre de 2024, una operación coordinada por Europol y Ameripol resultó en la detención de 17 personas en seis países, incluido Ecuador. Esta red se dedicaba a desbloquear teléfonos móviles robados y acceder a la información personal de los propietarios mediante técnicas de phishing, afectando a más de 480.000 víctimas en países como Chile, Colombia, Ecuador, Perú, España y Argentina. (Lorca & Viúdez, 2024)

CARACTERIZACIÓN DEL DELITO

El modelo de **Ciberdelincuencia como Servicio (CaaS)** ha ganado terreno en Ecuador, alineándose con una tendencia global en la que las actividades delictivas se comercializan como servicios. Esta modalidad no solo facilita la ejecución de ataques cibernéticos sofisticados, sino que también amplía el acceso a herramientas ilícitas a personas sin conocimientos técnicos avanzados, democratizando así la comisión de ciberdelitos. Frente a este panorama, es crucial adoptar medidas preventivas que permitan anticiparse a las amenazas y reducir la exposición a riesgos cibernéticos.

El **Convenio de Budapest**, ratificado por Ecuador mediante el Decreto Ejecutivo No. 332 del 12 de julio de 2024, establece un marco normativo integral para la cooperación internacional en la lucha contra los ciberdelitos. Este tratado, considerado como la norma internacional más completa hasta la fecha, proporciona a Ecuador las herramientas jurídicas necesarias para enfrentar fenómenos emergentes como la **Ciberdelincuencia como Servicio (CaaS)**, ofreciendo un enfoque estructurado sobre la persecución de ciberdelitos y la protección de la evidencia digital y electrónica. La adhesión al Convenio no solo refuerza las capacidades nacionales para tipificar y sancionar ciberdelitos, sino que también mejora la cooperación interinstitucional, permitiendo una respuesta coordinada frente a la creciente amenaza que representa la ciberdelincuencia globalizada, particularmente los servicios ilícitos comercializados en mercados digitales clandestinos. Así, el Convenio de Budapest se convierte en un pilar fundamental para la modernización de la legislación ecuatoriana y el desarrollo de estrategias preventivas en la lucha contra los ciberdelitos.

Si bien el **Código Orgánico Integral Penal (COIP, 2014)** contempla sanciones para los ciberdelitos, Ecuador aún ocupa el puesto 12 en la región en términos de legislación penal en el ámbito de las TIC. Esta posición refleja la necesidad urgente de fortalecer el marco normativo desde un enfoque preventivo, acompañado de estrategias de sensibilización, educación digital y cooperación interinstitucional. La escasa denuncia por parte de las víctimas y la limitada articulación entre instituciones dificultan una respuesta efectiva. Por ello, se recomienda avanzar hacia una cultura de ciberseguridad preventiva mediante campañas de concientización ciudadana, capacitación técnica y mecanismos eficaces de coordinación para mitigar el impacto de la ciberdelincuencia en el país. (Ponce M., 2024)

Perfilamiento del criminal

El CaaS ha universalizado la ciberdelincuencia, aumentando la cantidad de delitos informáticos y creando un ecosistema global con tácticas cada vez más sofisticadas.

Desde una perspectiva criminológica, esta descentralización ha diversificado el perfil del ciberdelincuente, alejándose de la figura del hacker individual y llevándolo a un modelo estructurado con roles específicos, similar al funcionamiento de las organizaciones delictivas tradicionales (Moya & Leticia, 2021) (Miró Llinares, 2023). En este contexto, se observa una división del trabajo que incluye desarrolladores de software malicioso, intermediarios que venden accesos ilegales, ejecutores de ataques y lavadores de activos digitales (Sutherland & Cressey, 2022).

Este fenómeno no solo plantea nuevos retos en la prevención y persecución de delitos informáticos, sino que también resalta la necesidad de actualizar los marcos jurídicos y las estrategias de cooperación internacional para mitigar su impacto (Orbit, 2024) (Miró Llinares, 2023).

Doctrina Jurídica Aplicada al Perfil del Ciberdelincuente

El Derecho Penal Informático ha evolucionado en los últimos años para adaptarse a la naturaleza dinámica de la ciberdelincuencia, particularmente en el modelo de Ciberdelincuencia como Servicio (*Cybercrime as a Service*, CaaS). Desde una perspectiva criminológica, el CaaS ha facilitado la especialización dentro de las estructuras delictivas, permitiendo que grupos organizados operen con un modelo de negocios similar al de las empresas legales, con roles específicos (Holt, 2023).

En Ecuador, la normativa vigente contempla la persecución de estos delitos dentro del Código Orgánico Integral Penal (COIP), el cual establece diversas sanciones para los delitos que atentan contra la seguridad de los activos de los sistemas de información y comunicación, tipificados en los siguientes artículos:

- **Artículo 229.-** Revelación ilegal de base de datos.
- **Artículo 230.-** Interceptación ilegal de datos.
- **Artículo 231.-** Transferencia electrónica de activo patrimonial.

- **Artículo 232.-** Ataque a la integridad de sistemas informáticos.
- **Artículo 233.-** Delitos contra la información pública reservada legalmente.
- **Artículo 234.-** Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.
- **Artículo 234.1.-** Falsificación informática.

A estos delitos se suman los que son cometidos con el uso de las TIC y que afectan a distintos bienes jurídicos protegidos, algunos de los cuales son:

- **Artículo 103.-** Pornografía con utilización de niñas, niños o adolescentes
- **Artículo 104.-** Comercialización de pornografía con utilización de niñas, niños o adolescentes
- **Artículo 166.-** Acoso sexual (ciberacoso)
- **Artículo 168.**- Distribución de material pornográfico a niñas, niños y adolescentes
- **Artículo 173.-** Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos
- **Artículo 178.-** Violación a la intimidad.

Desde el ámbito doctrinario, la teoría del control social de Gottfredson y Hirschi (Gottfredson & Hirschi, 2023) sostiene que la ciberdelincuencia se ve favorecida por la percepción de anonimato y la baja probabilidad de captura. En este sentido, la falta de mecanismos efectivos de supervisión digital y la sofisticación de las herramientas empleadas por los delincuentes cibernéticos han generado un entorno donde la impunidad se vuelve un factor determinante en la proliferación de estos delitos (Maimon & Louderback, 2023).

Por otro lado, la teoría de la racionalidad criminal aplicada al ciberespacio plantea que los ciberdelincuentes tomen decisiones basadas en un análisis de costo-beneficio, donde la facilidad de acceso a herramientas ilícitas y la alta rentabilidad de los ataques superan los riesgos legales asociados (Newman & Clarke, 2022). Esta perspectiva resalta la importancia de estrategias de prevención que incluyan la desarticulación de redes de CaaS y la implementación de sanciones más severas para desincentivar la participación en estos esquemas.

Caracterización del Ciberdelincuente en el Modelo CaaS

El modelo CaaS ha transformado el panorama de la ciberdelincuencia, permitiendo que cualquier individuo participe en actividades delictivas mediante la adquisición de herramientas y servicios en mercados clandestinos. Según (Porras, 2023), los ciberdelincuentes que operan bajo este modelo pueden clasificarse en cuatro categorías principales:

- **Desarrolladores de herramientas**: Crean y comercializan ransomware, malware avanzado, exploits y kits de phishing en mercados clandestinos.
- **Distribuidores y revendedores**: venden credenciales robadas, bases de datos filtradas y accesos ilícitos a sistemas vulnerados.

- **Operadores de ataques**: utilizan herramientas adquiridas en la dark web para realizar fraudes financieros, espionaje corporativo y ataques de denegación de servicio (DDoS).
- **Lavadores de dinero**: Especializados en ocultar el origen de ingresos ilícitos a través de criptomonedas y sistemas financieros opacos.
- **Lavadores de dinero:** especializados en ocultar el origen de ingresos ilícitos mediante criptomonedas y sistemas financieros opacos.

El modelo CaaS ha impulsado la profesionalización del ciberdelito, permitiendo la especialización de los ciberdelincuentes aumentando la eficiencia y reduciendo riesgos. La disponibilidad de servicios como Ransomware como Servicio (RaaS) y Phishing como Servicio (PhaaS) ha facilitado el acceso a herramientas sofisticadas, disminuyendo las barreras de entrada para nuevos ciberdelincuentes (Bantula, 2025).

El uso de Inteligencia Artificial (IA) ha potenciado las actividades de ciberdelincuencia, como la creación de correos electrónicos del tipo phishing más realistas, generar código malicioso y buscar vulnerabilidades en aplicaciones específicas. Esto ha aumentado la efectividad y el alcance de las campañas maliciosas, permitiendo a los ciberdelincuentes engañar a sus víctimas de manera más convincente y evadir las defensas de seguridad tradicionales (Días, 2024).

En América Latina**,** el Informe sobre Ciberdelincuencia 2023 de Interpol señala un aumento de delitos vinculados al modelo CaaS en Ecuador, con mayor participación de actores locales en la distribución y monetización de datos robados (Interpol, 2023)**.**

Motivaciones y Factores de Riesgo

Las motivaciones de los ciberdelincuentes pueden explicarse mediante diversas teorías criminológicas:

Asociación Diferencial: sugiere que la conducta delictiva se aprende a través de la interacción con otros. En el contexto de la ciberdelincuencia, los individuos adquieren comportamientos delictivos mediante su participación en comunidades en línea, donde prevalecen normas y técnicas criminales (Sutherland & Cressey, 2022).

Actividades Cotidianas: indica que la delincuencia ocurre cuando convergen un delincuente motivado, una víctima vulnerable y la ausencia de un guardián capaz. En el ámbito digital, el fácil acceso a herramientas ilícitas y la proliferación de oportunidades en línea incentivan la comisión de delitos cibernéticos. (Cohen & Felson, 1979).

Desinhibición Digital: plantea que el anonimato y la invisibilidad en línea reducen las inhibiciones sociales y morales, facilitando comportamientos delictivos que los individuos podrían evitar en interacciones cara a cara. (Suler, 2024).

El anonimato, la descentralización y la alta rentabilidad de la ciberdelincuencia han impulsado un aumento significativo de los delitos cometidos mediante el uso de las TIC en el Ecuador.

El país registró un aumento del 4,9% en ciberdelitos en 2024, con el fraude digital y la suplantación de identidad como las actividades ilícitas más comunes (Universo, 2024).

Modus Operandi y Técnicas de Ataque

Los ciberdelincuentes que operan bajo el modelo CaaS siguen un enfoque estructurado en sus ataques, descrito a través del modelo de la Cyber Kill Chain, que consta de siete fases:

Reconocimiento: Recopilan información sobre el objetivo utilizando técnicas como ingeniería social principalmente y phishing selectivo para identificar vulnerabilidades.

Preparación: Desarrollan o adquieren herramientas maliciosas para explotar las vulnerabilidades identificadas.

Distribución: Implementan las herramientas maliciosas en los sistemas objetivo, a menudo mediante correos electrónicos de phishing o dispositivos infectados.

Explotación: Aprovechan las vulnerabilidades para obtener acceso no autorizado a los sistemas o datos.

Instalación: Instalan malware adicional o crean puertas traseras para mantener el acceso persistente.

Comando y control: Establecen canales de comunicación para controlar los sistemas comprometidos de forma remota.

Acciones sobre los objetivos: realizan actividades finales como exfiltración de datos, cifrado de información (ransomware) o destrucción de sistemas (Tarlogic, 2023) (INCIBE, 2020).

Implicaciones y desafíos

Implicaciones

Aumento de amenazas de ataques cibernéticos: Ecuador registra un incremento significativo de delitos cometidos con el uso de las TIC, Esto incluye ataques como ransomware, phishing avanzado y ataques a infraestructuras críticas facilitados por la venta de herramientas ilícitas en la dark web.

Impacto económico y social: Los ciberdelitos afectan a sectores estratégicos como el financiero, gubernamental, de las telecomunicaciones entre otros, estos son vulnerables a ataques organizados que pueden afectar significativamente en áreas económicas críticas y atentar contra la seguridad nacional.

Desafíos jurídicos y legislativos: A pesar de la existencia de regulaciones en el Código Orgánico Integral Penal (COIP), la rápida evolución de la ciberdelincuencia dificulta la aplicación efectiva de la ley.

Desafíos

Personal capacitado: a nivel mundial existe un déficit de profesionales en ciberinteligencia, ciberseguridad, forense digital y ciberdelincuencia, Ecuador no es la excepción; esta problemática global limita la capacidad de respuesta ante incidentes

Cooperación internacional: Ecuador es miembro de Ameripol e Interpol y el 12 de diciembre de 2024 depositó el instrumento de ratificación del Convenio de Budapest, la cooperación internacional es vital para enfrentar las amenazas cibernéticas de manera efectiva. Sin embargo, la falta de acuerdos sólidos y la ausencia de integración efectiva obstaculizan la lucha contra la ciberdelincuencia transnacional.

Concienciación y educación: promover la conciencia a toda la ciudadanía sobre los riesgos cibernéticos y fortalecer la educación así como la prevención en seguridad digital generando una cultura digital para reducir la vulnerabilidad de la población a todo nivel para lo cual se propone trabajar con el Ministerio de Educación y la Academia Superior.

SERVICIOS RELACIONADOS CON ACTIVIDADES ILÍCITAS EN EL ÁMBITO DIGITAL

Amenazas Cibernéticas

Entre los servicios de CaaS más demandados se encuentran las amenazas cibernéticas como el Malware (MaaS), Ransomware (RaaS) y los ataques de denegación de servicio distribuidos (DDoS).

Mercados ilícitos ofrecen a los delincuentes acceso a kits listos para usar, infraestructura para desplegar ataques masivos e incluso soporte técnico, popularizando el acceso a tecnologías criminales avanzadas.

La facilidad con la que se puede acceder a estas herramientas representa una amenaza significativa para individuos, empresas y gobiernos, destacando la urgencia de fortalecer las estrategias de prevención y respuesta ante la ciberdelincuencia organizada.

Oferta de Amenazas Cibernéticas

En mercados ilegales de la deep y dark web, se comercializan servicios ilícitos a través de interfaces profesionales y accesibles, similares a las de comercios electrónicos legítimos como por ejemplo los servicios onion.

A continuación, se presentan ejemplos reales de estas ofertas:

1. **Creación de Malware (MaaS)**

   Se ofrecen programas maliciosos a medida para infectar dispositivos y robar información sensible.

   Los precios oscilan entre 50 y 1000 dólares, dependiendo del tipo de malware y sus capacidades.

2. **Ataques DDoS por Encargo**

   Los ciberdelincuentes brindan la posibilidad de lanzar ataques de Denegación de Servicio Distribuido (DDoS) contra sitios web o redes, dejándolos inaccesibles.

   Los precios comienzan en $10 dólares por una hora de ataque.

3. **Kits de Phishing (PhaaS)**

   Se venden herramientas y plataformas automatizadas de phishing que incluyen plantillas de correos electrónicos y páginas web fraudulentas diseñadas para engañar a las víctimas y robar credenciales bancarias, datos personales y otra información confidencial

   Se comercializan por $50 dólares, permitiendo a cualquier persona realizar ataques de phishing.

4. **Botnets como Servicio**

   Se ofrece el acceso a redes de dispositivos infectados (botnets) para lanzar ataques masivos, distribuir spam o realizar fraudes en línea.

   Los precios oscilan entre $20 y $200 dólares, dependiendo del tamaño de la botnet y su capacidad de ataque.

5. **Exploits de Día Cero**

   Se comercializan vulnerabilidades desconocidas para los desarrolladores, permitiendo a los atacantes explotarlas antes de que sean parcheadas.

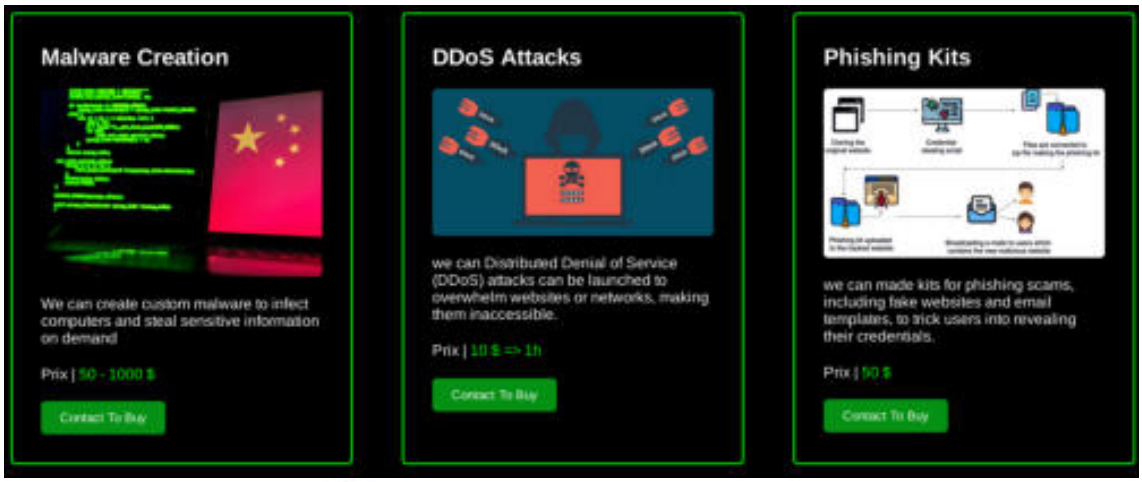
   Los precios varían desde $5000 hasta $10,000 dólares, dependiendo de la criticidad del exploit.

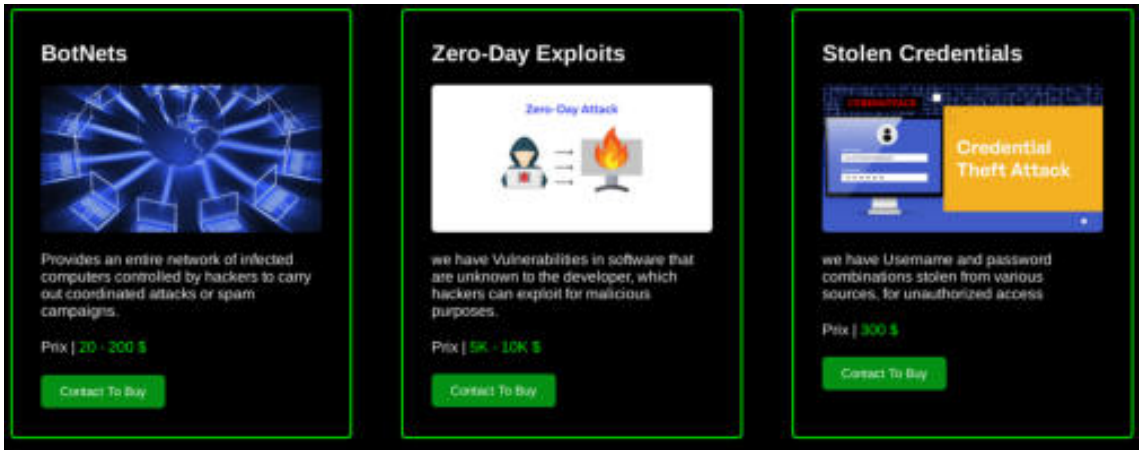
6. **Credenciales Robadas**

   Bases de datos con combinaciones de nombres de usuario y contraseñas obtenidas de filtraciones y ataques previos.

   Se venden por $300 dólares, facilitando el acceso no autorizado a cuentas personales y empresariales.

Imagen 4: *Oferta de servicios ilícitos en la Dark Web / Deep Web*





Estos servicios reflejan la creciente profesionalización de la ciberdelincuencia como servicio, donde se pueden acceder a herramientas altamente sofisticadas para cometer delitos.

CIBERDELINCUENCIA COMO SERVICIO: CASOS Y MERCADO EN LA DARK WEB

Plataformas Financieras

LabHost

La plataforma LabHost un servicio de Phishing-as-a-Service (PhaaS) permitía ejecutar ataques de phishing automatizados; su principal objetivo era el robo de credenciales bancarias de usuarios en Canadá, EEUU y otros países. Ofrecía más de 40 plantillas que imitaban páginas de inicio de sesión de instituciones financieras; permitiendo gestionar

campañas fraudulentas desde una única interfaz y contaba con LabRat, una herramienta que intercepta códigos de dos factores (2FA) en tiempo real. Además, brindaba servicio de soporte y estadísticas, para perfeccionar los métodos delictivos de ataque.

EvilProxy

Es otra plataforma de PhaaS diseñada para permitir a ciberdelincuentes robar credenciales bancarias y evadir autenticación de dos factores (2FA) mediante ataques de intermediario (AiTM, Adversary-in-the-Middle). Su uso ha aumentado significativamente en ataques contra bancos y fintechs, facilitando accesos fraudulentos a cuentas protegidas con MFA (Multi-Factor Authentication) ofrece un panel de control para gestionar ataques, estadísticas en tiempo real y métodos para evadir la detección de sistemas de seguridad.

Según informes de SISA Infosec[1] y Sekoia.io[2], esta amenaza ha sido una de las más peligrosas para el sector financiero en 2023.

Grandoreiro

Troyano bancario de origen latinoamericano utilizado para robar credenciales financieras y datos personales de usuarios en Brasil, México, España y Argentina. Se propaga principalmente a través de correos electrónicos de phishing o enlaces fraudulentos diseñados para engañar a las víctimas e infectar sus dispositivos.

Emplea diversas técnicas de evasión, como ofuscación de código y cifrado de comunicaciones con sus servidores de comando y control (C&C). Entre sus funcionalidades incluyen la capacidad de registrar las pulsaciones del teclado, capturar credenciales bancarias en tiempo real y mostrar ventanas emergentes falsas que imitan las interfaces de bancos legítimos para engañar a los usuarios.

Evil Corp y Dridex

Evil Corp es un grupo de ciberdelincuentes especializado en Malware-as-a-Service (MaaS), responsable del desarrollo y distribución de Dridex, un troyano bancario utilizado para robar credenciales financieras y realizar fraudes electrónicos. Una vez infectado el dispositivo captura credenciales bancarias, registra pulsaciones de teclado y manipula transferencias electrónicas además permite a los atacantes tomar control remoto de los dispositivos infectados, facilitando la ejecución de fraudes sin que la víctima lo detecte.

Venta de tarjetas de crédito en la Deep Web/ Dark Web

Los mercados ilegales en la dark web permiten adquirir tarjetas bancarias clonadas y prepagadas de diversas entidades como Visa, MasterCard y American Express, entre otras. Estas tarjetas suelen estar asociadas a fraudes financieros y actividades de lavado de dinero

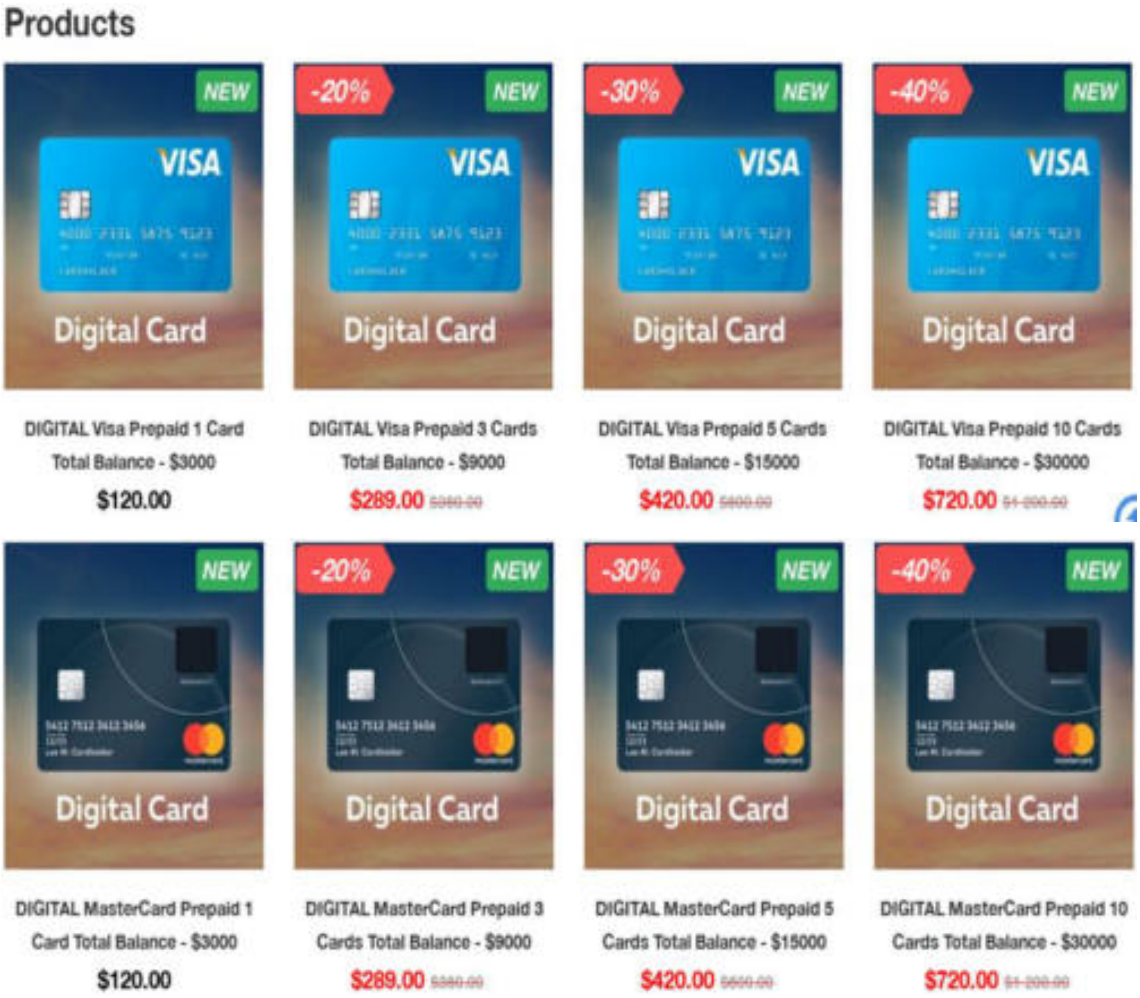
[1] SISA es una empresa global de soluciones de ciberseguridad impulsada por la ciencia forense https://www.sisainfosec.com/

[2] Sekoia.io Empresa europea de ciberseguridad que ofrece soluciones de detección y respuesta extendidas (XDR) https://www.sekoia.io/en/homepage/

y se venden a precios significativamente bajos en comparación con su supuesto saldo disponible.

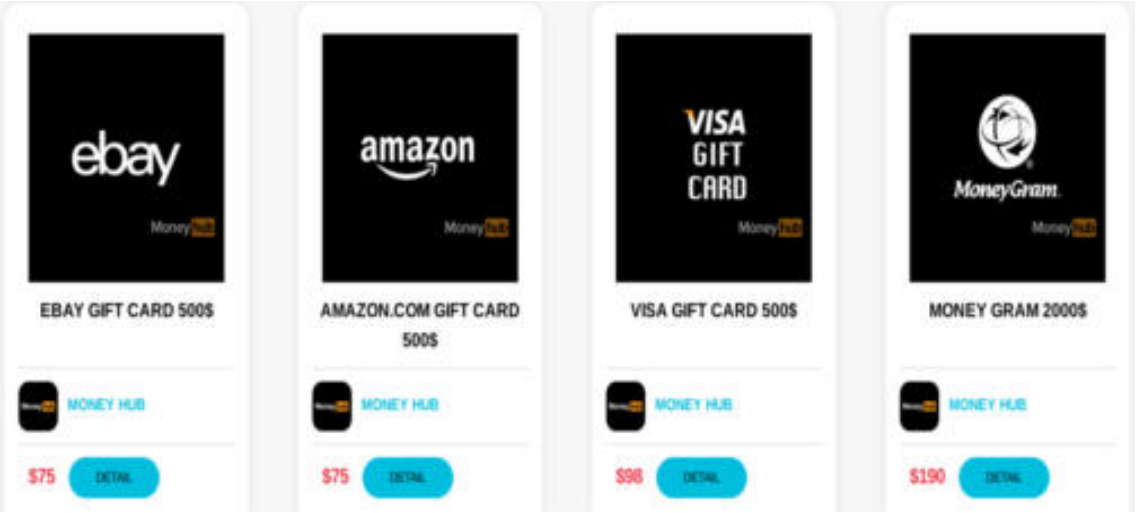
Los valores de saldo en estas tarjetas varían entre $1,500 y $30,000 USD, mientras que los precios de venta oscilan entre $65 y $720 USD, dependiendo del monto disponible y la cantidad adquirida. Se ofrecen descuentos por volumen, incentivando la compra masiva de tarjetas fraudulentas. Además, existen diferentes categorías con límites de retiro diario y otras sin restricciones, lo que facilita su uso en esquemas fraudulentos (Imagen 5).

Imagen 5: *Oferta de tarjetas de crédito en la Dark Web / Deep Web*



Estos mercados ilegales también incluyen la venta de tarjetas de regalo de plataformas como Amazon, eBay y MoneyGram, además de servicios ilegales de transferencia de dinero a través de Western Union, PayPal y Skrill, que pueden ser utilizados para el blanqueo de fondos obtenidos ilícitamente.

Imagen 6: *Oferta de tarjetas de crédito en la Dark Web / Deep Web*



Plataformas para Hackeo de Redes Sociales

Los ciberdelincuentes ofrecen sus habilidades y conocimientos para comprometer Redes Sociales a cambio de dinero. (Vincent, 2018).

Funcionamiento del modelo de negocio.

1- **Propuesta de valor**: Obtención de información privilegiada e información de competidores o a su vez la recuperación de cuentas comprometidas con anterioridad.

2- **Segmento de clientes**: Son las personas y empresas con interés de conseguir una ventaja competitiva en el mercado o a su vez simplemente obtener información sensible.
3- **Canales**: Únicamente se le puede encontrar en sitios de la Dark web.
4- **Relaciones con clientes**: Servicio personalizado y confidencial a los clientes, incluyen soporte técnico 24/7, informes detallados, promesas de confidencialidad y anonimato.
5- **Fuentes de ingreso**: Especialmente pagos por servicio, es decir, los pagan por cada servicio efectuado.
6- **Recursos clave:** Equipos de hackers experimentados y especializados en redes sociales, herramientas y software de hacking avanzados, infraestructura de servidores y redes seguras.
7- **Actividades clave:** Anonimato en la ejecución del servicio, análisis y entrega de la información sensible de una manera comprensible.
8- **Estructura de costos**: Generalmente costos de infraestructura, en el caso de tiendas el proveedor debe cancelar una tarifa específica para poder ofrecer sus servicios a través de la plataforma.

Para este análisis, se clasificó a las páginas web objeto de estudio en dos categorías: sitios web independientes y tiendas/mercados.

Plataformas Sitios web independientes

Páginas creadas por ciberdelincuentes para obtener réditos económicos, ofrecen servicios para comprometer sistemas, vulnerar claves de acceso y extraer información sensible de redes sociales.

Tabla 3: *Páginas ofertando servicios de hacking para Redes sociales*

Red social Sitio Web	Facebook	Whatsapp	Twitter/X	Instagram	Snapchat	Tiktok	Youtube
Shadow Hacker	$200	$260	$200	$200	$200	$260	$200
#Z#	$270	$225	$225	$270	$225	-	-
Find a Hacker	$400	$500	$350	$400	$300	-	$400
Injection Team	$200	$200	$200	$200	$200	$200	$200

Fuente: El ciberdelito como servicio: una amenaza creciente (Cena & Liang, 2023)

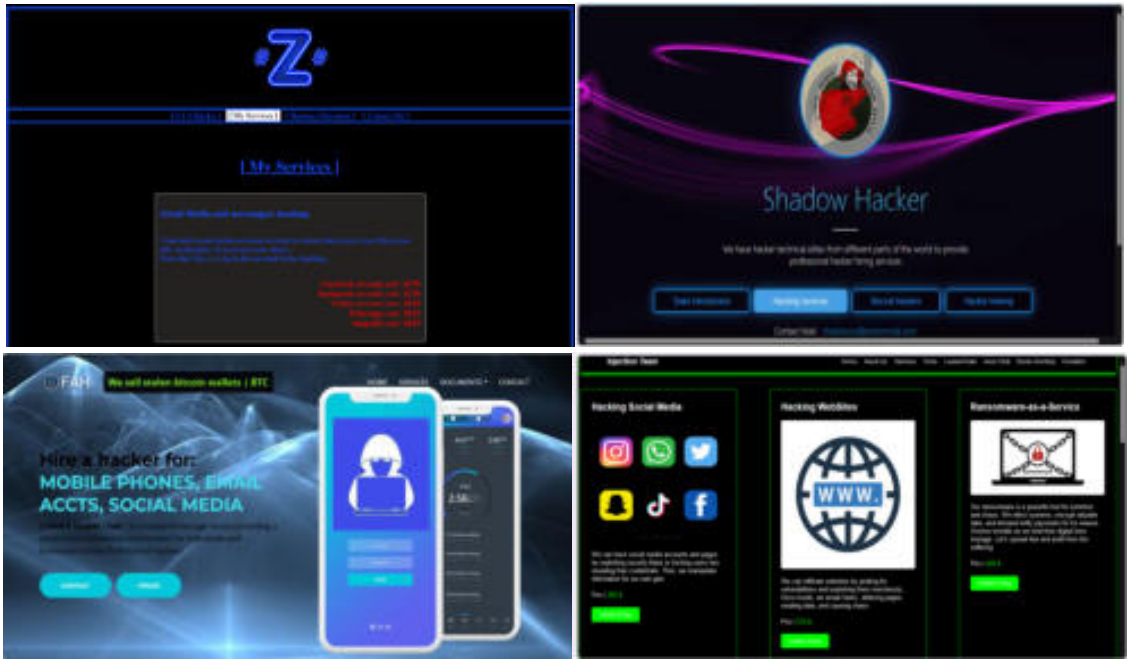
En estos sitios el ciberdelincuente establece las condiciones, métodos de pago y datos de contacto para entablar una comunicación directa permitiendo órdenes personalizadas según los requerimientos. .

Puntos importantes en un Sitio web Independiente

- El único medio de contacto es vía correo electrónico por razones de seguridad.

- Los servicios son prepagos, por anticipo o también se puede optar por el servicio de “depósito en garantía” que se refiere a la injerencia de terceros. Intermediarios externos que retienen y regulan el pago de los fondos requeridos para dos partes involucradas en una transacción determinada, asegurando que solo se complete cuando se cumplan todas las condiciones acordadas.
- Algunas transacciones independientemente pueden ser realizadas en la web abierta (clearnet).
- Reembolso total del dinero anticipado recibido en caso de no cumplir con los requisitos específicos del cliente.
- Las comunicaciones son encriptadas, tunelizadas a través de VPN y transportadas a través de la red Tor.
- Los perpetradores garantizan confidencialidad. Una vez finalizado un pedido, se elimina definitivamente toda la conversación mantenida por correo electrónico o cualquier otro medio de comunicación, así como cualquier tipo de información que se pudiese haber almacenado previamente para la ejecución del servicio.
- El método de pago es mediante criptomonedas como: Bitcoin, Monero, Litecoin y Ethereum.

Imagen 7: *Páginas usadas objeto de estudio*



Plataformas Tiendas / Mercados

Webs diseñadas se enfocan esencialmente en el anonimato de los usuarios; ofrecen funcionalidades como reales con carrito de compras, procesamiento de pagos en línea y una experiencia de compra integrada. Los ciberdelincuentes también han encontrado en estas plataformas para potenciar estos ilícitos.

Los mercados ilegales para vulnerar servicios en redes sociales según Joshua Cena varían en su precio según el tipo de ataque entre $125 y $249 (dólares americanos) en las diferentes plataformas mostradas a continuación:

Tabla 4: *Tiendas/Mercados ofertando servicios de hacking para redes sociales*

Red Social / Sitio Web	Facebook	Whatsapp	Twitter/X	Instagram	Snapchat	Tiktok	Telegram
Deep Market	$199	$199	$199	$199	$199	$199	$199
DarkBay	$249	$200-249	$225	$170-249	$249	$249	$200
Rent a Hacker	$125	$250	$125	$125	$150	$150	$150
E-Market	$125	$150	$125	$125	-	$150	$125

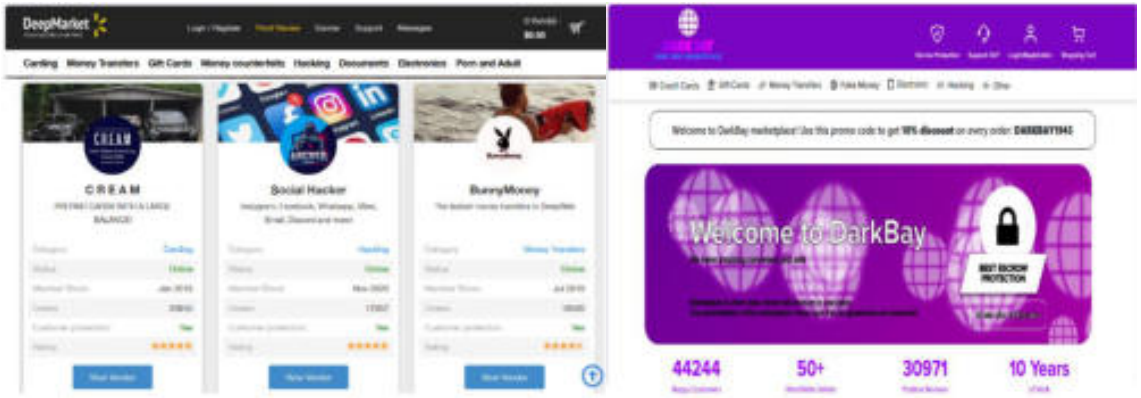
Fuente: El ciberdelito como servicio: una amenaza creciente (Cena & Liang, 2023)

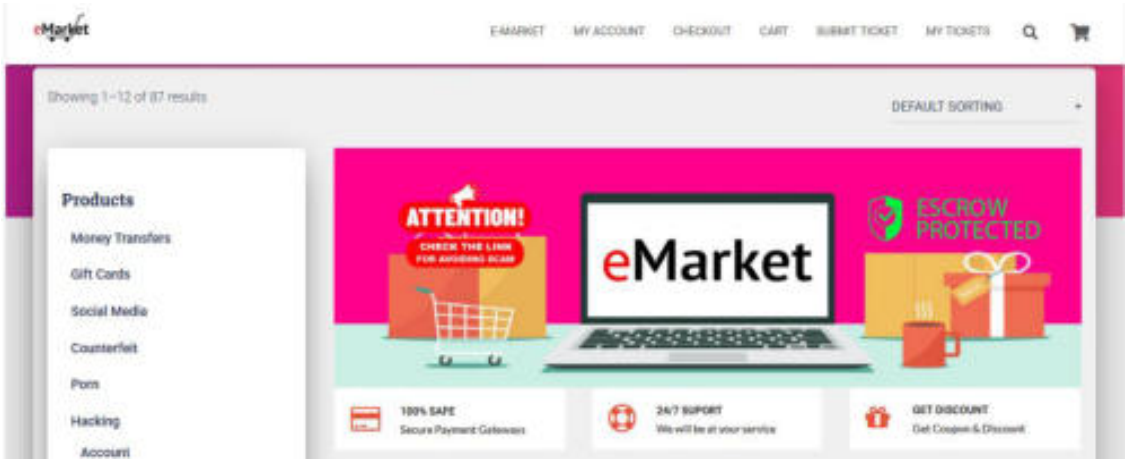
Puntos fundamentales de una Tienda

- Las plataformas digitales tienes características que describimos a continuación Su página de inicio es muy similar a los sitios de comercio electrónico convencionales como Amazon, Walmart o Flipkart con banners completos, productos destacados, etc.
- Permiten crear una cuenta de usuario con la cual se podrá realizar las compras e irlas almacenando en el carrito hasta que se decida proceder con el pago.
- Brindan información de los vendedores (ciberdelincuentes), como el estado en línea, la fecha de inscripción, número de ventas, la calificación y si ofrecen protección al comprador o no. Esto permitiría a los usuarios encontrar fácilmente a los proveedores más confiables y establecidos que a los estafadores potenciales más nuevos.
- Emplean un sistema de depósito en garantía multiforma 2-3. Esto se traduce a que una transacción solo se habilitará si dos de las partes involucradas (contratante delictivo-tienda-proveedor) la autorizan. Esto asegura que ninguna de las partes pueda estafar a la otra y que las transacciones se realicen de manera justa.
- Ofrecen servicio ininterrumpido al contratante delictivo incluyendo asesorías para el proceso de pago.
- El comprador puede iniciar una disputa en caso de que el producto no satisfaga sus necesidades y al igual el vendedor también puede iniciar una disputa en caso de que el producto haya sido entregado al contratante delictivo (mediante pruebas) y éste no libere el dinero del depósito en garantía.

- Al ser una plataforma que reúne a múltiples proveedores, el mercado se vuelve diverso, lo que permite acceder a una variedad de precios para el mismo servicio.
- Mantienen los mismos métodos de pago, priorizando las criptomonedas, especialmente Bitcoin.
- Al igual que los sitios web independientes las tiendas también ofrecen la confidencialidad e integridad de los datos al manejar la información de manera encriptada.

Imagen 8: *Tiendas / Mercados usados para el estudio*





Fuente: *Dark Web / Deep Web*

Acciones del Ministerio del Interior y la Policía Nacional contra la ciberdelincuencia

Ministerio del Interior

El Ministerio del Interior a través de la Dirección de Ciberdelitos realiza acciones de prevención y combate a la ciberdelincuencia mediante la generación de política pública y estrategias, que permitan al país desde un enfoque integral y estructurado, hacer frente a este fenómeno; para lo cual se desarrollan propuestas de planes, programas, proyectos, instrumentos técnico-científicos, técnico-legales y mecanismos o convenios de cooperación nacional e internacional, mismos que permiten dar una respuesta efectiva a las necesidades de seguridad digital de la ciudadanía. Algunas de las acciones realizadas incluyen:

Campaña del Plan de Concienciación Sobre Delitos Informáticos que Atentan Contra la Integridad de Niños, Niñas y Adolescentes

El "*Plan de Concienciación Sobre Delitos Informáticos que Atentan Contra la Integridad de Niños, Niñas y Adolescentes"* se apunta en crear una comunidad informada y empoderada, alrededor de los niños, niñas y adolescentes, que reconozca los riesgos de los delitos cometidos con el uso de las TIC que afectan a este grupo etario, de tal forma que se cuente con las herramientas para prevenir y proteger a los menores de edad en los entornos digitales.

En relación a lo anterior se creó la campaña en las redes sociales del Ministerio del Interior que tiene como objetivo sensibilizar y educar a la comunidad para prevenir y combatir los ciberdelitos y delitos cometidos con uso de las tecnologías que afectan a menores de edad.

Imagen 9: *Campaña del Plan de Concienciación sobre Delitos Informáticos que Atentan Contra la Integridad de Niños, Niñas y Adolescentes*

Fuente: *Ministerio del Interior*

Protocolo de actuación para investigación en fuentes abiertas digitales.

La Dirección de Ciberdelitos trabajó en una propuesta para el uso y aplicación de metodología de “Inteligencia en fuentes abiertas” – OSINT, de tal forma que sirva de apoyo institucional a las distintas áreas en la búsqueda de información digital relevante de acuerdo con sus actividades y competencias.

El Protocolo de Actuación de Búsqueda de Información en Fuentes Abiertas Digitales es una guía metodológica diseñada para estandarizar y fortalecer las capacidades técnicas y operativas de los servidores públicos y elementos policiales en la búsqueda de información digital en fuentes abiertas como plataformas web, redes sociales, blogs entre otras, información pública que puede ser relevante para la prevención de posibles delitos o para su investigación, e incluso para la toma de decisiones de nivel jerárquico, administrativo y

operativo. Este protocolo proporciona directrices sobre la identificación, recolección, análisis y preservación de información digital, garantizando que estos procedimientos se realicen de manera legal, ética y profesional, y que puedan ser utilizados en los procesos judiciales seguidos por la Fiscalía.

Guía práctica para el Ciberpatrullaje

Guía práctica orientada a los agentes policiales que realizan patrullaje en el ciberespacio, de tal forma que pueda detectar indicios de posibles ciberdelitos o actos sospechosos en línea; se están realizando las gestiones para la expedición mediante Acuerdo Ministerial.

Instructivo para la Preservación de Información Publicada en Redes Sociales y Páginas Web.

La Dirección de Ciberdelitos trabaja en el análisis de información para la elaboración del "Instructivo para la Preservación de Información Publicada en Redes Sociales y Páginas Web.", el cual se encuentra orientado para uso del personal que realiza el análisis de la información contenida en redes sociales y páginas web, este instructivo, detalla los métodos adecuados de preservación bajo las mejores prácticas técnicas y legales.

Guía de Buenas Prácticas para la Prevención de la Ciberdelincuencia en Establecimientos de Turismo.

Debido al aumento en el uso de las tecnologías y las nuevas tendencias en el cometimiento de delitos, mediante cooperación interinstitucional entre la Dirección de Ciberdelitos del Ministerio del Interior (MDI) y la Dirección de Protección al Usuario de Servicios Turísticos del Ministerio de Turismo (MINTUR), se elaboró *"Guía de Buenas Prácticas para la Prevención de la Ciberdelincuencia en Establecimientos de Turismo".* Este documento aborda la prevención de delitos cometidos con el uso de las TIC en establecimientos de turismo, presentando estrategias aplicables tanto para las empresas del sector como para los usuarios que hacen uso de los servicios que permitan prevenir y enfrentar este tipo de ilícitos de manera efectiva. La Guía en su versión 1.0 fue entregada al MINTUR para su difusión.

En este contexto, se destaca el papel fundamental de la Dirección de Ciberdelitos del Ministerio del Interior, que trabaja arduamente a través de planes, proyectos y programas especializados para prevenir, detectar y combatir estas amenazas. Su labor constituye un pilar esencial en el combate a la ciberdelincuencia, promoviendo un entorno digital más seguro para todos.

Unidad Nacional de Ciberdelito de la Policía Nacional

Según el TCnl. García Cataña Héctor Gonzalo Jefe de la Unidad Nacional de Ciberdelito de la Policía Nacional la acciones que realizan se describen a continuación:

El avance de la tecnología ha generado nuevas oportunidades de desarrollo social, así como también nuevas formas de criminalidad, donde los ciberdelitos han adquirido relevancia en el contexto nacional e internacional. Lo anterior concuerda con Pérez et al (2018), que menciona que el auge de las tecnologías digitales ha generado nuevas formas de gestión de la información digital, la cual es accesible para las personas.

Este artículo analiza la evolución de la ciberdelincuencia en Ecuador, donde se ha registrado un aumento en delitos como el fraude digital, la violencia en línea y el abuso de menores en entornos virtuales. En este contexto, la Unidad Nacional de Ciberdelito (CIBERPOL) desempeña un rol clave en la detección, investigación y mitigación de estos ilícitos.

Panorama de la Ciberdelincuencia en Ecuador

La ciberdelincuencia ha crecido en los últimos años debido al aumento del acceso a internet y la digitalización de servicios bancarios y administrativos. Según datos de la Unión Internacional de Telecomunicaciones (UIT), en 2023 el 87% de la población ecuatoriana tenía acceso a internet, lo que ha incrementado las oportunidades para la comisión de delitos cibernéticos (UIT, 2023).

En este sentido, entendiendo que los ciberdelitos son conductas típicas, antijurídicas, y punibles, que tienen como fin el uso indebido de las TIC, el ciberdelito se clasifica en ciberdependientes y ciberhabilitantes.

Ciberdependientes: Aquellos que solo pueden cometerse mediante el uso de tecnologías digitales, ya que dependen de ella completamente. Ejemplos: phishing, ransomware, acceso no autorizado a sistemas y el robo de datos.

Ciberhabilitantes: Son delitos donde la tecnología se utiliza como un medio para cometer la infracción. Incluyen el fraude digital, la estafa en línea, el ciberacoso y la suplantación de identidad.

La Unidad Nacional de Ciberdelito en Ecuador, su estructura y funcionamiento

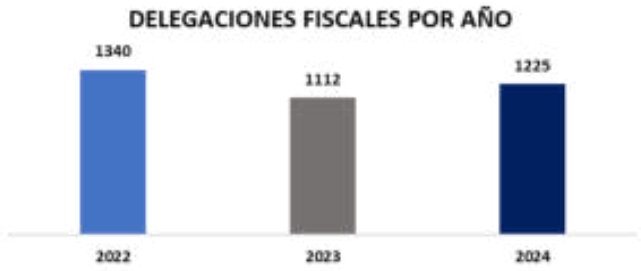
Para garantizar una respuesta efectiva, Ecuador cuenta con la Unidad Nacional de Ciberdelito, conformado por 37 servidores policiales altamente especializados, distribuidos estratégicamente en diversos departamentos, con funciones específicas orientadas a la investigación, prevención y combate de actividades ilícitas en el entorno digital, siendo sus áreas:

- Sección de Fraude Digital: Investiga estafas en línea, suplantación de identidad y delitos financieros cometidos mediante plataformas electrónicas.
- Sección de Violencia Digital: Atiende casos de acoso en línea, extorsión y explotación infantil, protegiendo a las víctimas de agresiones en entornos digitales.
- Sección de Incidentes Informáticos: Aborda ataques cibernéticos, intrusiones en sistemas y vulneraciones de seguridad digital.

- Sección de Ciberpatrullaje: Monitorea redes sociales y plataformas en busca de actividades ilícitas.
- Departamento de Análisis de la Información: Examina datos para identificar patrones delictivos.
- Departamento de Coordinación Operacional: Supervisa y ejecuta operativos.
- Departamento de Apoyo Operativo: Administra funciones administrativas y documentales.
- Departamento Jurídico: Asegura que las investigaciones digitales cumplan con la normativa vigente.

Esta estructura ha permitido gestionar una importante carga procesal con 1 225 delegaciones en el año 2024, 113 delegaciones más que el año anterior 2023 que existieron 1 112 delegaciones fiscales, según muestra la figura a continuación.

Tabla 5: *Carga procesal de la Unidad al 31 de diciembre de 2024.*



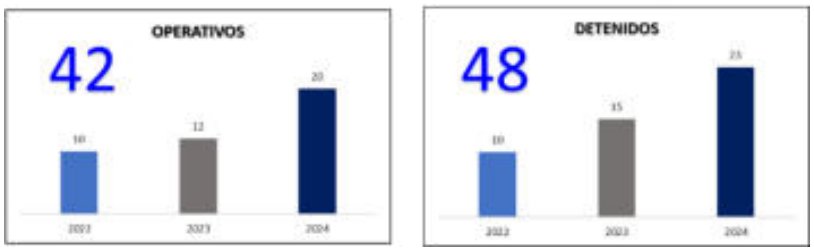
Fuente: *DAI/CIBERPOL*

De igual manera la Unidad Nacional de Ciberdelito ha logrado obtener excelentes resultados que evidencian un incremento sostenido en la ejecución de operativos y la detención de presuntos delincuentes en los últimos tres años. El número de operativos realizados pasó de 10 en 2022 a 20 en 2024, lo que representa un aumento del 100%, reflejando un fortalecimiento en las capacidades de investigación y respuesta ante delitos digitales. De manera correlativa, el número de detenidos también ha mostrado una tendencia creciente, pasando de 10 en 2022 a 23 en 2024, lo que equivale a un incremento del 130%.

Estos avances destacan el compromiso de la Unidad en la lucha contra la ciberdelincuencia, fortaleciendo estrategias de inteligencia, coordinación interinstitucional y acciones preventivas que permitan garantizar la seguridad en el entorno digital ecuatoriano.

Tabla 6: *Resultados operativos de la Unidad al 31 de diciembre de 2024.*

Resultados operativos de la Unidad



Fuente: *DAI/CIBERPOL*

Principales Desafíos en la Lucha contra la Ciberdelincuencia

Falta de Denuncias: Uno de los principales problemas en la lucha contra la ciberdelincuencia es la baja tasa de denuncias. Muchas víctimas no reportan los delitos por desconocimiento o desconfianza en el sistema judicial, lo que genera una percepción errónea sobre la disminución del fenómeno (ONU, 2023).

Evolución y Sofisticación de los Delitos: El ciberdelito no desaparece, sino que evoluciona constantemente, adaptándose a nuevas tecnologías y vulnerabilidades. En 2024, la ciberdelincuencia ha mutado hacia modalidades más sofisticadas, como los ataques de ransomware dirigidos específicamente a empresas y entidades gubernamentales, el uso de inteligencia artificial y deepfakes para la comisión de fraudes financieros avanzados, y la extorsión digital mediante la filtración de datos como mecanismo de chantaje. Estos cambios evidencian la necesidad de actualizar continuamente las estrategias de defensa cibernética para mitigar los riesgos emergentes y fortalecer la seguridad digital.

Educación y Concienciación: A pesar de las campañas de concienciación, persisten brechas en la educación digital, sin embargo, la Unidad Nacional de Ciberdelito ha capacitado a más de 15.000 personas en seguridad digital bajo la iniciativa "Ciberespacio: Riesgos y Seguridad en el Mundo Digital". Sin embargo, es necesario fortalecer la alfabetización digital en sectores vulnerables para reducir la incidencia delictiva (CIBERPOL, 2024).

Estrategias para Enfrentar la Ciberdelincuencia en Ecuador

Para mitigar la creciente amenaza del ciberdelito, Ecuador debe adoptar una estrategia más agresiva basada en cuatro pilares clave:

Fortalecimiento Legal y Regulación: Tipificar nuevos delitos digitales, incluyendo fraudes con inteligencia artificial y ataques a infraestructuras críticas.

Endurecer sanciones para ciberdelincuentes y mejorar la cooperación con organismos internacionales.

Educación y Cultura de Ciberseguridad: Incluir ciberseguridad en la educación básica y universitaria.

Promover campañas de alfabetización digital dirigidas a ciudadanos y empresas.

Implementar sistemas de detección temprana de amenazas en instituciones bancarias y gubernamentales y fomentar la adopción de herramientas de seguridad digital, como autenticación multifactor y cifrado de datos.

Inversión en Tecnología y Protección Digital: Incentivar a empresas y organismos públicos a mejorar sus protocolos de seguridad. Implementar centros nacionales de ciberseguridad para monitoreo y respuesta a incidentes.

Cooperación Internacional: Ecuador debe continuar fortaleciendo la colaboración con Interpol, Europol y otras agencias internacionales para rastrear y capturar a ciberdelincuentes que operan desde el extranjero.

Conclusión

La ciberdelincuencia es un problema en constante evolución, impulsado por el avance tecnológico y la digitalización de la sociedad. Si bien Ecuador ha tomado medidas significativas para enfrentar esta amenaza, aún persisten desafíos en materia de denuncias, sofisticación de los ataques y educación en ciberseguridad.

Para garantizar un entorno digital seguro, es imprescindible que Ecuador fortalezca su marco normativo, incremente la inversión en ciberseguridad y fortalezca la cooperación internacional. La lucha contra la ciberdelincuencia no se trata solo de reducir cifras, sino de proteger a la sociedad en un mundo cada vez más interconectado con cultura de ciberseguridad.

PERSPECTIVA DE EXPERTOS EN CIBERDELINCUENCIA

La Ciberdelincuencia como Servicio en Ecuador: Perspectivas y Desafíos en la Lucha contra el *Ransomware*

Dr. Fierro Fierro Christian Alex

Juez del Tribunal de Garantías Penales, especializado para el juzgamiento de delitos de corrupción y crimen organizado

Resumen

La ciberdelincuencia como servicio (CaaS, por sus siglas en inglés) ha evolucionado como un modelo delictivo que permite la comercialización de herramientas y servicios para cometer ciberdelitos. En Ecuador, el ransomware ha emergido como amenaza dentro de este

esquema, afectando tanto a instituciones públicas como privadas. La reciente adhesión de Ecuador a la Convención de Budapest ofrece una oportunidad para fortalecer la prevención, investigación y sanción de estos delitos.

Palabras clave: ciberdelincuencia, ransomware, ciberespacio, Convención de Budapest

Introducción

La globalización y el avance de las tecnologías de la información y comunicación (TIC) han transformado el mundo, facilitando la comunicación, rompiendo fronteras y reduciendo los tiempos de respuesta. Sin embargo, estas innovaciones también han creado nuevas oportunidades para que las organizaciones delictivas aprovechen la anonimidad y el alcance del ciberespacio, lo que les permite realizar actividades criminales con menor riesgo de detección.

El ciberespacio, un espacio digital donde las personas interactúan, comparten información y realizan diversas actividades en línea, ha cambiado las dinámicas de las relaciones económicas, políticas, sociales y personales ((Barrio, Delitos 2.0: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018). Este término, acuñado por primera vez en la novela de ciencia ficción Neuromancer de William Gibson (1984), se refiere a un mundo virtual paralelo al físico donde se pueden realizar muchas actividades que anteriormente solo eran posibles en el mundo real. (Scotti, 2016)

Sin embargo, en la actualidad, la ciberdelincuencia es una realidad que no la podemos desconocer ya que su accionar amenaza al mundo entero. Afectando a personas naturales, jurídicas e inclusive a gobiernos. La búsqueda constante de métodos para obtener dinero fácil al margen de la legalidad o en su defecto cumplir sus propios caprichos por parte de quienes delinquen, ha permitido que vayan a la par con el desarrollo tecnológico utilizando sus bondades, lo que ha dado cabida al incremento de la ciberdelincuencia como servicio, permitiendo que personas con fines delincuenciales adquieran herramientas tecnológicas avanzadas sin necesidad de conocimientos que requieran sofisticidad.

Los ciberdelincuentes recurren a diversos métodos para lograr sus objetivos ilícitos. Entre estos se encuentran el *phishing*, técnica empleada para obtener de manera fraudulenta credenciales de acceso; los *spyware*, programas diseñados para recopilar información sin el conocimiento del usuario; los *rootkits*, herramientas que facilitan el acceso remoto a un sistema sin la autorización del propietario; y los *ransomware*, programas que restringen el acceso a los sistemas afectados y exigen un pago para su desbloqueo. Además, estos actores malintencionados utilizan diferentes estrategias informáticas y variantes de *malware* con el propósito de acceder ilícitamente a sistemas informáticos, modificarlos o destruir sus componentes. (Barrio, Ciberdelitos 2.0 Amenazas criminales del ciberespacio, 2020)

El Ransomware en el Ciberespacio

El delito de extorsión ha existido desde hace mucho tiempo, pero con la llegada del entorno digital, ha evolucionado y adquirido nuevas formas como el uso de *malware* para llevar a cabo ataques cibernéticos. Un ejemplo de ello es el *ransomware,* un software malicioso que bloquea o cifra la información de un equipo o dispositivo y exige un pago para su recuperación. En consecuencia, no se puede hablar de una nueva forma de delinquir sino más bien de una evolución utilizando las ventajas que ofrece el ciberespacio.

Al establecer un símil con el tipo penal de extorsión, tipificado y sancionado en el artículo 185 del Código Orgánico Integral Penal (COIP), en el que una persona es obligada a realizar un acto o efectuar un pago en perjuicio de su patrimonio, se observa una situación similar en el ataque a la integridad de sistemas informáticos, contemplado en el artículo 232 del mismo cuerpo normativo. Este delito, cuando se comete a través del ransomware, implica la retención o encriptación de información, exigiendo un pago para su liberación, lo que refleja una evolución del fenómeno extorsivo en el entorno digital.

En los últimos años la Región ha sido objeto de varios ataques cibernéticos específicamente en la modalidad de ransomware. Entre octubre de 2023 y octubre de 2024, se bloquearon aproximadamente alrededor de 560,000 ataques de ransomware (Kaspersky, 2024)Y claro el Ecuador, no es ajeno a esta realidad un caso emblemático ocurrido en 2021, con la Corporación Nacional de Telecomunicaciones (CNT) que fue objeto de un ataque cibernético lo cual dejó en evidencia que los ciberdelincuentes no tienen fronteras para lograr sus objetivos.

Impacto de la Adhesión de Ecuador a la Convención de Budapest

El Convenio de Budapest sobre Ciberdelincuencia representa un hito importante en los esfuerzos internacionales para combatir los delitos cibernéticos. La adhesión de Ecuador al Convenio, aunque es un paso positivo, plantea interrogantes sobre la capacidad del país para implementar efectivamente sus disposiciones. Las reformas al Código Orgánico Integral Penal en 2023 demuestran un esfuerzo por alinear la legislación nacional con los estándares internacionales (Asamblea Nacional del, 2023) Sin embargo, estas reformas podrían no ser suficientes para abordar las complejidades tecnológicas y jurisdiccionales del cibercrimen transnacional. (Fierro, 2024)

Conclusión

El *ransomware* representa una amenaza creciente en la región, y Ecuador no ha sido la excepción. Por ello, es fundamental impulsar programas de capacitación que fortalezcan la capacidad de la sociedad para prevenir los riesgos asociados a los ataques cibernéticos y responder de manera eficiente ante su ocurrencia. Una reacción inmediata y coordinada, informando de inmediato a las autoridades competentes, como la Fiscalía de Ciberdelitos y Ciberpol, resulta clave para mitigar el impacto de estos delitos.

Finalmente, es importante recordar que la prevención y la capacitación de los usuarios del ciberespacio constituyen las herramientas más eficaces para hacer frente a los ciberdelincuentes. Para ello, resulta esencial la adopción de normas estrictas de ciberseguridad y el tratamiento de estos riesgos con la debida seriedad y prioridad

La ciberdelincuencia como servicio CaaS

Mgs. Jorge Mauricio Néjer Guerrero

Especialista de Ciberdelitos Dirección de ciberdelitos del Ministerio del Interior, Perito informático y Perito electrónico

La ciberdelincuencia como servicio (CaaS) ha transformado el panorama del ilícito en el entorno digital, permitiendo que actores con variadas motivaciones y mínimos conocimientos técnicos puedan ejecutar ataques sofisticados. Este modelo, inspirado en esquemas empresariales del *software como servicio SaaS*, aprovecha avances tecnológicos como la hiperconectividad, las redes de datos y las herramientas de inteligencia artificial (IA) para expandir sus operaciones, poniendo en riesgo la seguridad ciudadana y económica a escala mundial. El CaaS es un modelo de negocio para la delincuencia organizada en línea en el que profesionales de tech (o "proveedores") ofrecen capacidades de ciberataque o modalidades de ciberdelito a los clientes, a menudo por suscripción. Los clientes encuentran el tipo de servicio que desean y luego pagan una tarifa de suscripción o alguna comisión, casi siempre a través de criptomonedas preservando el anonimato y es aquí también donde la ciberdelincuencia ha encontrado un aliado estratégico, las criptomonedas, para operar con impunidad y escalar sus actividades a nivel global. Estas monedas digitales, diseñadas inicialmente para transacciones seguras, han sido cooptadas por redes criminales que aprovechan sus características técnicas para fines ilícitos.

Evolución tecnológica y estructura del CaaS

El CaaS opera mediante plataformas en la *dark web* donde se comercializan servicios ilícitos como **ransomware**, **phishing** y **ataques DDoS**, usando criptomonedas para transacciones anónimas. (Ganguli, 2024) (Field Effect, 2024)

Su estructura jerárquica incluye:

- **Desarrolladores**: Crean herramientas maliciosas (ej. ransomware personalizable).
- **Intermediarios**: Gestionan mercados digitales y pagos en criptoactivos.
- **Clientes**: Desde individuos hasta organizaciones criminales que alquilan estos servicios.

Este modelo ha profesionalizado el ciberdelito, registrando un crecimiento del 300% en ataques por suscripción entre 2022 y 2025. (Kerner, 2025)

En el **Ransomware como servicio (RaaS)** el 98% de los rescates por *ransomware* se pagan en criptomonedas, principalmente Bitcoin. (Incibe, 2019) Casos emblemáticos como

WannaCry demostraron cómo el CaaS comercializa herramientas de secuestro digital con soporte técnico incluido. Los atacantes exigen pagos en monederos cifrados que ocultan su identidad, usando *mixers,* para "lavar" las transacciones antes de convertirlas a divisas tradicionales. (Financial Crime Academy, 2025)

Hiperconectividad y redes de datos: multiplicadores de riesgo

La expansión de IoT y 5G ha facilitado:

- **Ataques coordinados**: Botnets de dispositivos inteligentes para inundar redes (ej. 1.5 millones de ataques DDoS diarios en 2024). (Colacicco, 2023)
- **Ingeniería social avanzada**: Uso de datos de LinkedIn y redes sociales para crear campañas de spear-phishing hiperpersonalizadas. (Ankit, 2024)
- **Infiltración en cadenas de suministro**: Compromiso de software legítimo para distribuir malware, como el caso SolarWinds en EE.UU. (Kerner, 2025)

Lavado de capitales criminales

Las criptomonedas permiten:

Movimiento transfronterizo instantáneo de fondos ilícitos sin intermediarios bancarios (Ardila, 2022)

Uso de *tumblers* (servicios de mezcla) que fragmentan transacciones en múltiples carteras (Financial Crime Academy, 2025)

Integración con mercados de la *dark web* para compra de drogas, armas o datos robados (Taboada, 2019).

Infraestructura criminal en la dark web

Plataformas como Sinbad operan como "bancos sombra" para organizaciones criminales, cobrando comisiones del 2-5% por transacción (Financial Crime Academy, 2025)

Foros clandestinos ofrecen servicios llave en mano: desde *phishing kits* hasta ataques DDoS, con pagos en Monero o Zcash (Paesano, 2025)

Inteligencia Artificial: el acelerador del crimen digital

La IA ha potenciado el CaaS mediante:

Tabla 6: *Carga procesal de la Unidad al 31 de diciembre de 2024.*

Aplicación	Impacto	Ejemplo
Generación de contenido	Phishing convincente mediante GPT-4	Campañas en español con 98% de precisión (Check Point Team, 2024)
Optimización de ataques	Análisis en tiempo real de vulnerabilidades	Ataques BGP dirigidos a rutas críticas (Colacicco, 2023)
Evasión de detección	Malware que muta según defensas del objetivo	Ransomware *Polimórfico AI-Enhanced* (Check Point Team, 2024)

Fuente: *Dirección de Ciberdelitos*

En 2024, el 67% de los ciberataques emplearon herramientas basadas en IA, incluyendo *deepfakes* para suplantar ejecutivos en videollamadas. (Check Point Team, 2024)

Casos regionales: crimen organizado y CaaS

Europa

- **Hacktivismo**: Grupos como *Anonymous* usan DDoS-as-a-Service contra gobiernos (ej. ataques a infraestructuras energéticas alemanas en 2023). (Ganguli, 2024)
- **Lavado de activos**: Plataformas como *Sinbad* mezclan criptomonedas de ransomware con fondos legales, moviendo €4.3 billones en 2024. (Field Effect, 2024)
- **Lavado de corrupción política:** Operación "Tulipán Blanca" en España (Taboada, 2019)

Estados Unidos

- **Narcotráfico digital**: Carteles mexicanos contratan servicios de *stalkerware* para vigilar agentes fronterizos. (Tal, 2024)
- **Triple extorsión**: Ransomware-as-a-Service (RaaS) contra hospitales, combinando cifrado de datos, filtración de información y ataques DDoS. (Kerner, 2025)
- **Ransomware a hospitales:** Ataque a Colonial Pipeline (2021): $4.4M en BTC (Incibe, 2019)

Latinoamérica

- **Mineria ilegal**: Botnets infectan sistemas industriales para extraer criptomonedas (ej. ataque a Petrobras en 2024 que desvió 15% de capacidad computacional). (Tal, 2024)
- **Narcotráfico 4.0**:
    - *México*: Cárteles usan CaaS para hackear sistemas logísticos de puertos. (Tal, 2024)
    - *Financiamiento de carteles narcos: Cárteles mexicanos usando BTC para compra de armas (Ardila, 2022)*
    - *Brasil*: Mega-filtración de datos de 220 millones de personas facilitó extorsiones masivas en 2023. (Tal, 2024)
    - *Costa Rica*: Ataques ransomware coordinados por grupos rusos paralizaron el sistema fiscal por semanas. (Tal, 2024)

Estas técnicas emergentes incluyen el uso de *wallets* falsas que drenan fondos de usuarios (Incibe, 2019), y brokers OTC que facilitan conversión a efectivo sin KYC (Financial Crime Academy, 2025). La combinación de CaaS con criptomonedas ha creado un ecosistema donde hasta grupos criminales tradicionales, subcontratan capacidades cibernéticas, pagando en monedas digitales por servicios de hackeo, espionaje o lavado. (Paesano, 2025) (Taboada, 2019)

Este panorama exige respuestas coordinadas: desde regulaciones blockchain que permitan trazabilidad sin comprometer privacidad, hasta la adopción de herramientas IA para detectar patrones de lavado en tiempo real (Financial Crime Academy, 2025) (Paesano, 2025). La

naturaleza global del fenómeno hace imprescindible la cooperación entre agencias de ciberseguridad y unidades financieras internacionales.

En el Ecuador si bien es cierto se han hecho esfuerzos desde la revisión y actualización del marco normativo que desembocó en la adhesión del país al Convenio sobre la Ciberdelincuencia (Budapest), hace falta mucho por recorrer en el desarrollo de política pública adecuada acorde a las exigencias de las nuevas tecnologías como el blockchain, cryptos, computación cuántica, Internet of Things (IoT), tecnologías OT, IA, entre otras, mismas que exigen un alto nivel de conocimientos del talento humano tanto en áreas técnico científicas como inversión en equipamiento y herramientas especializadas a fin de prevenir y combatir ilícitos inherentes al fenómeno de la ciberdelincuencia. Según datos de la Fiscalía General del Estado quien es la encargada de la investigación Penal, la Apropiación fraudulenta por medios electrónicos Código Orgánico Integral Penal (COIP) Art. 190 es el más denunciado con 18055 casos, seguido de la Violación a la intimidad Art. 178 con 9201 casos y la Estafa por medios electrónicos Art. 196 numerales 1 y 2 con 4434 casos, un dato no menor es el Acceso No consentido a un Sistema Informático con 2626 casos. **(Imagen 1).**

La pregunta es: ¿el sistema de investigación y justicia está preparado para realizar la adecuada investigación y judicialización de estos casos? La respuesta es NO, esto obedece a varios factores como talento humano especializado, inversión en infraestructura tecnológica, generación de cultura digital, programas de concienciación social, entre otros analizados en las distintas mesas de trabajo realizadas con las instituciones como son FGE, Consejo de la Judicatura, Policía Nacional, MINTEL, ARCOTEL, Defensa, Defensoría Pública, Ministerio de Educación y la Academia. Es así que la Dirección de Ciberdelitos del Ministerio del Interior trabaja en la creación de planes programas y proyectos para prevenir y combatir el fenómeno de la ciberdelincuencia, proyectos como la Estrategia Nacional contra la Ciberdelincuencia, el Plan de Concienciación para Niños Niñas y Adolescentes, El Proyecto de Centro Cibernético de la Policía Nacional, el Proyecto de Plataforma de Gobernanza Digital para Gestión Técnico Científico Forense de la Policía Nacional, El Manual de Actuación para la recolección, preservación, tratamiento y análisis de evidencia digital así como convenios internacionales, instructivos de herramientas y planes de capacitación básicos y especializados en ciberdelincuencia, ciberinteligencia y forense digital son proyectos relevantes impulsados desde la Dirección a fin de mejorar las capacidades del estado y principalmente de la Policía Nacional y cambiar el paradigma que exige la investigación de delitos de alta tecnología, con acciones articuladas entre las instituciones del estado, la empresa privada y la cooperación internacional al tratarse de delitos que no contemplan fronteras y se desarrollan en un ciberespacio cada vez más complejo.

Imagen 9: *Noticias del Delito de los delitos cometidos con el uso de las TIC*

Fuente: *Sistema estadístico Dirección de Ciberdelitos*

Conclusión

El CaaS representa una amenaza sistémica que requiere cooperación internacional y marcos regulatorios ágiles y efectivos. Su combinación con IA, redes 5G y economía digital ha creado un ecosistema donde el crimen organizado tradicional se retroalimenta de herramientas cibernéticas, escalando riesgos desde el robo de identidad hasta el sabotaje de infraestructuras críticas. La respuesta efectiva debe integrar las nuevas tecnologías como la inteligencia artificial defensiva, legislación transnacional sobre criptoactivos, capacitación estatal especializada y capacitación ciudadana en la acción de la ciberdelincuencia.

CIFRAS Y ESTADÍSTICAS DE DELITOS COMETIDOS CON EL USO DE LAS TIC

A continuación, se presentan las cifras relacionadas con los delitos cometidos con el uso de las TIC, cuyas fuentes son la Fiscalía General del Estado, la Unidad Nacional de Ciberdelito de la Policía Nacional y el Consejo de la Judicatura.

Los datos obtenidos de la Fiscalía General del Estado, corresponden a las noticias de delito que recibe dicha Institución. Según la Fiscalía, una noticia de delito hace referencia a una denuncia de un presunto hecho delictivo[3]. La Fiscalía puede delegar las investigaciones

[3] *Gob.ec. Recuperado el 15 de agosto de 2024* https://www.fiscalia.gob.ec/recepcion-de-denuncias-de-delitos-comunes/

al organismo especializado de la Policía Nacional o a otros del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses.

Los datos correspondientes a la Unidad Nacional de Ciberdelito de la Policía Nacional (Ciberpol) son de las delegaciones que recibe por parte de la Fiscalía, para investigar y actuar en relación con el hecho delictivo reportado.

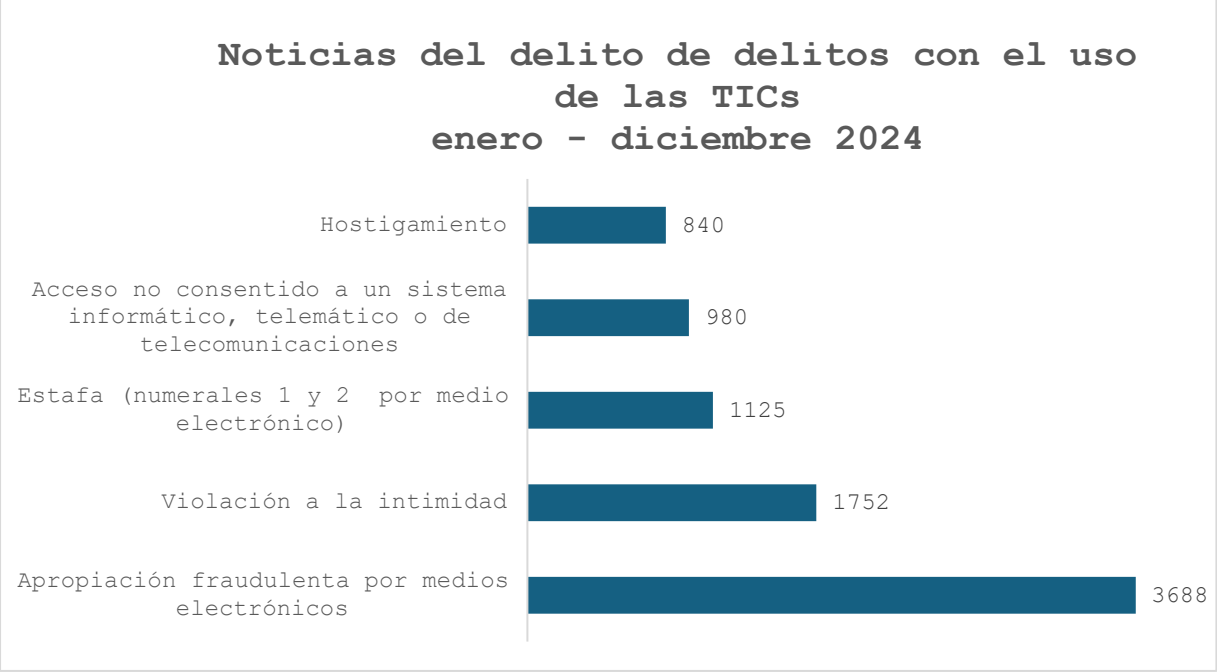
Respecto al Consejo de la Judicatura las cifras son de las causas ingresadas y resueltas que se presentan ante el sistema judicial del país, ya sea de delitos remitidos por la Fiscalía o de contravenciones presentadas directamente en las Unidades Judiciales.

Fiscalía General del Estado

Una vez realizado el análisis de los datos estadísticos correspondientes a las Noticias de Delito (NND) proporcionados por la Dirección de Estadísticas y Sistemas de la Información de la Fiscalía General del Estado, se determinó que, en el periodo comprendido entre enero y diciembre de 2024, se registraron un total de **9,459** Noticias de Delito relacionadas con delitos cometidos con el uso de las TIC.

A continuación, se presentan las cinco Noticias de Delito de delitos con el uso de las TIC más representativas de este período.

Gráfico 1: *Top 5 de noticias del delito registradas por delito*



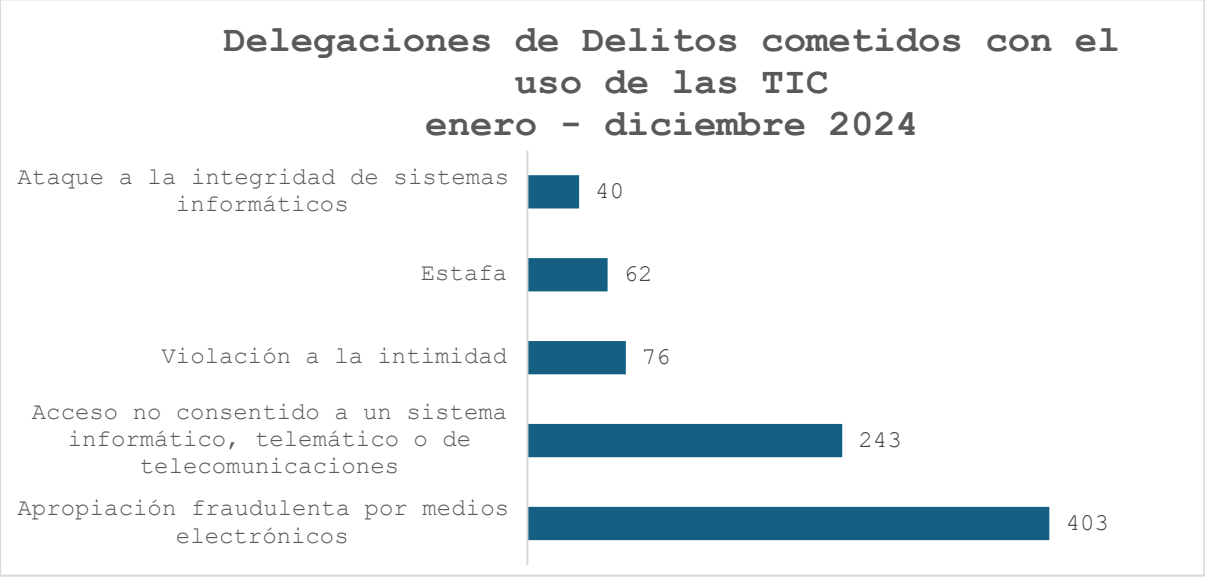
Fuente: *Fiscalía General del Estado*

Policía Nacional

La información estadística proporcionada por la Unidad Nacional de Ciberdelito de la Policía Nacional, refleja las delegaciones enviadas por la autoridad competente durante el período comprendido de enero a diciembre de 2024, registrando un total de **938** delegaciones por delitos cometidos con el uso de las TIC.

A continuación, se presentan las delegaciones de delitos cometidos con el uso de las TIC más representativas de este período.

Gráfico 2: *Delegaciones de delitos cometidos con el uso de las TIC enero – diciembre 2024*



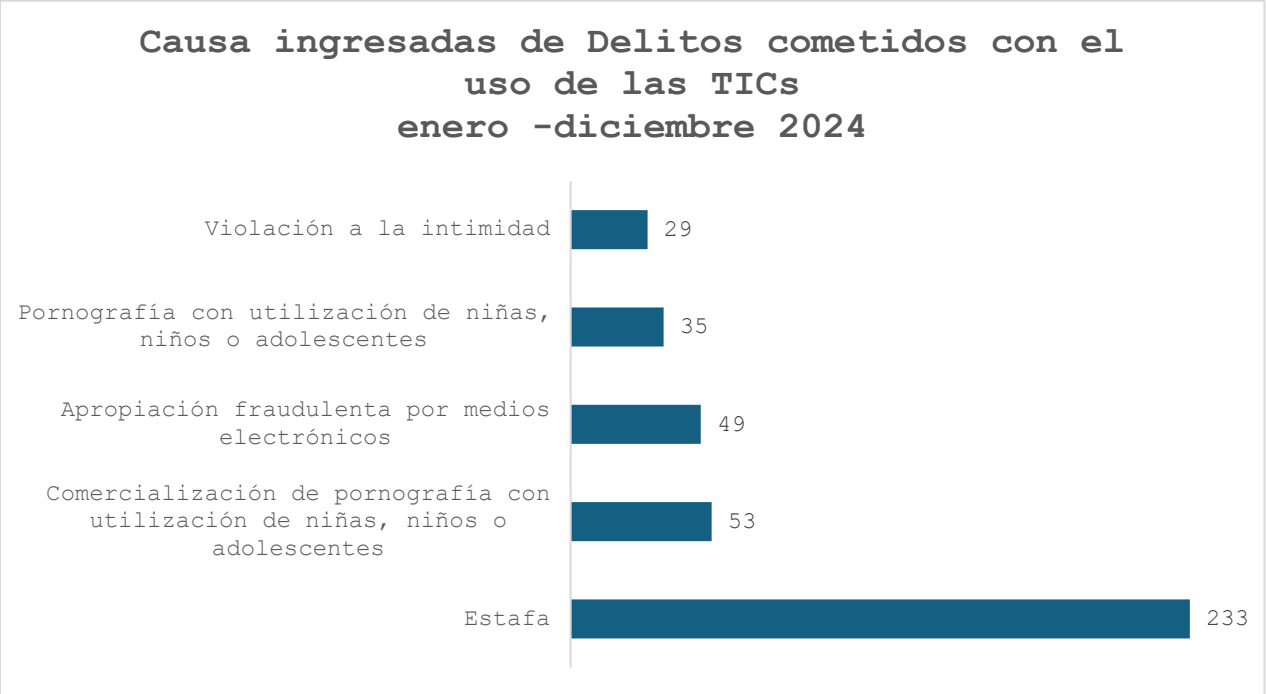
Fuente: *Unidad Nacional de Ciberdelito de la Policía Nacional*

Consejo de la judicatura

A continuación, se presentan las estadísticas sobre las causas ingresadas y resueltas en el ámbito de los delitos cometidos con el uso de las TIC, según los datos de la Función Judicial, correspondientes al período de enero a diciembre de 2024. Durante este tiempo, se registraron un total de 447 causas ingresadas, de las cuales 180 fueron resueltas.

A continuación, se presentan las causas ingresadas de Delitos con el uso de las TIC más representativas de este período.

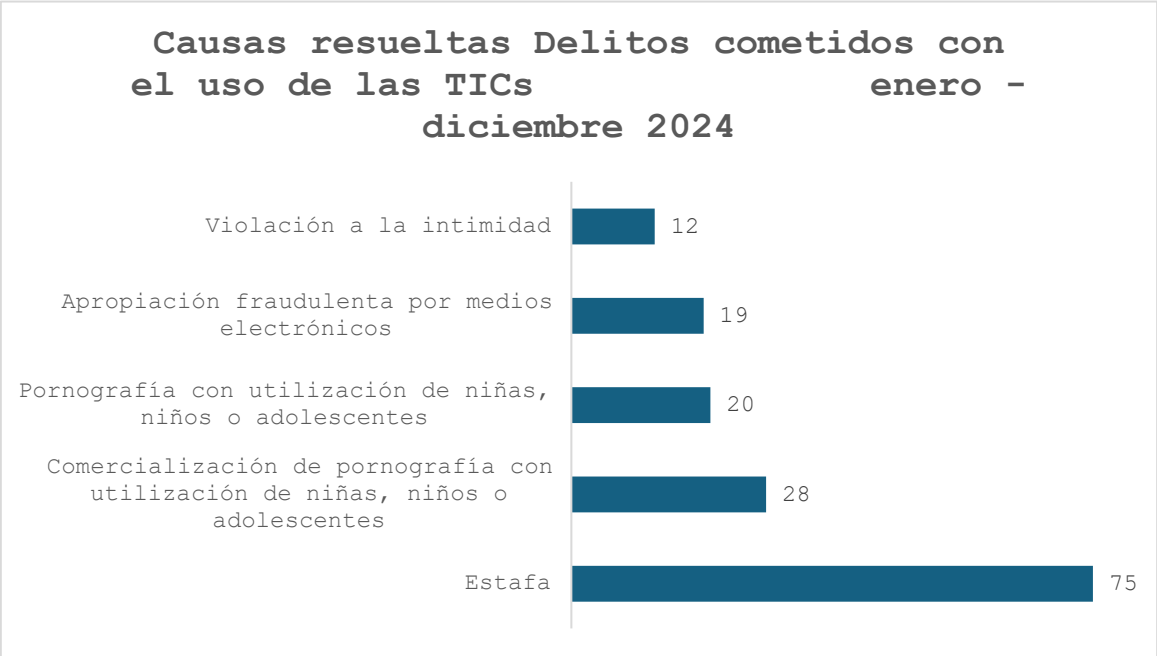
Gráfico 3: *Top 5 Causas ingresadas a la función judicial*



Fuente: *Consejo de la Judicatura*

A continuación, se presentan las causas resueltas de Delitos con el uso de la TIC más representativas de este período.

Gráfico 4: *Top 5 Causas ingresadas de la función judicial*



Fuente: *Consejo de la Judicatura*

CONCLUSIONES

- La ciberdelincuencia se ha convertido en un problema social en constante evolución, impulsado por el avance tecnológico y la digitalización de la sociedad. Para combatir este fenómeno delictivo y garantizar un entorno digital seguro, Ecuador ha ejecutado medidas significativas como el fortalecimiento de su marco normativo, consolidación de las unidades especializadas para investigación, capacitación permanente, programas de educación y concienciación, cooperación nacional e internacional, entre otros; sin embargo, estas acciones deben fortalecerse para combatir estas amenazas de constante evolución para garantizar la protección de los ciudadanos y del Estado ante los peligros del ciberespacio.
- La proliferación del modelo de Ciberdelincuencia como Servicio (CaaS) en Ecuador demanda fortalecer las medidas preventivas mediante educación digital, campañas de concienciación ciudadana y mejoras en la cooperación interinstitucional, para anticiparse a las amenazas emergentes en el ciberespacio.
- La adhesión de Ecuador al Convenio de Budapest constituye una oportunidad estratégica para modernizar el marco normativo nacional, promover una cultura de ciberseguridad

preventiva y establecer mecanismos más sólidos de respuesta ante la creciente amenaza de la ciberdelincuencia globalizada.

- El surgimiento de plataformas como LabHost y EvilProxy demuestra la urgente necesidad de fortalecer las estrategias de prevención frente al phishing y al robo de credenciales, priorizando la capacitación en buenas prácticas digitales y el uso de métodos de autenticación robustos.
- La actividad de troyanos bancarios como Grandoreiro y Dridex subraya la importancia de implementar campañas masivas de sensibilización ciudadana, promover el uso de soluciones de seguridad actualizadas y reforzar la detección temprana de amenazas para reducir el impacto de fraudes electrónicos en el país.

Bibliografía

Allodi, L. C. (2015). Then and now: On the maturity of the cybercrime markets the lesson that black-hat marketeers learned. *IEEE Transactions on Emerging Topics in Computing*, 35-46.

Alto, P. (2025, abril). *What is malware vs. Ransomware?* Retrieved from rom https://www-paloaltonetworks-com.translate.goog/cyberpedia/what-is-malware-vs-ransomware?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wa

Ankit, A. (2024, Septiembre 03). *Navigating the rising tide of cybercrime in a hyper-connected world*. Retrieved from https://etedge-insights.com/technology/cyber-security/navigating-the-rising-tide-of-cybercrime-in-a-hyper-connected-world/

Ardila, S. (2022, abril 25). *Monedas digitales y ciberdelito*. Retrieved from https://www2.deloitte.com/co/es/pages/risk/articles/monedas-digitales-y-ciberdelito.html

Asamblea Nacional del, E. (2023). *Reformas al Código Orgánico Integral Penal (COIP).* Retrieved from https://www.asambleanacional.gob.ec

Bantula, E. (2025, 2). *La Ciberdelincuencia: Hacia una Profesionalización y Rentabilidad Sin Precedentes* . Retrieved from https://www.worldcomplianceassociation.com/3325/articulo-la-ciberdelincuencia-hacia-una-profesionalizacion-y-rentabilidad-sin-precedentes-.html

Barrio, M. (2018). *Delitos 2.0: Aspectos penales, procesales y de seguridad de los ciberdelitos.* Editorial Jurídica.

Barrio, M. (2020). *Ciberdelitos 2.0 Amenazas criminales del ciberespacio.* Editorial Jurídica.

Bocconi. (2025, 01 21). *Los ciberincidentes en Latinoamérica aumentaron 25% cada año en la última década.* Retrieved from https://www.welivesecurity.com/es/cibercrimen/ciberincidentes-america-latina-aumentaron/

Cena, J., & Liang, W. (2023, 12). *Cybercrimen as a Service a Growing Threat.* Retrieved from https://www.researchgate.net/scientific-contributions/Joshua-Cena-2303902580

Check Point Team. (2024, Febrero 1). *Generative AI is the Pride of Cybercrime Services*. Retrieved from https://blog.checkpoint.com/research/generative-ai-is-the-pride-of-cybercrime-services/

Cloudflare. (2025, abril 25). *What is a DDoS attack?* Retrieved from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, pp. 588-608.

Colacicco, D. (2023, Mayo 04). *The impact of AI on cybercrime*. Retrieved from https://www.anapaya.net/blog/the-impact-of-ai-on-cyber-crime

Días, C. (2024, Noviembre 13). Retrieved from El auge de la IA dispara los ciberataques en el sector financiero en 2024: https://cincodias.elpais.com/smartlife/lifestyle/2024-11-13/el-auge-de-la-ia-dispara-los-ciberataques-en-el-sector-financiero-en-2024.html

Field Effect. (2024, Septiembre 26). *The rise of cybercrime-as-a-service*. Retrieved from https://fieldeffect.com/blog/cybercrime-as-a-service

Fierro, C. (2024). *El delito de pornografía infantil en el Ecuador: dificultades investigativas (Tesis de maestría).* Retrieved from http://dspace.udla.edu.ec/handle/33000/16477

Financial Crime Academy. (2025, Marzo 26). *Comprender los métodos de lavado de dinero criptográfico: el delito de criptomonedas*. Retrieved from https://financialcrimeacademy.org/es/metodos-de-lavado-de-dinero-en-criptodivisas-la-clave-de-los-delitos-de-criptodivisas/

Freeze, D. (2018). Retrieved from Cybercrime To Cost The World $10.5 Trillion Annually By 2025: https://cybersecurityventures.com/ cybercrime-damages-6-trillion-by-2021/

Ganguli, P. (2024). The Rise of Cybercrime-as-a-Service: Implications and Countermeasures. *International Journal for Multidisciplinary Research*, 1-35.

Gatlan, S. (2024, noviembre 22). *Microsoft disrupts ONNX phishing-as-a-service infrastructure.* Retrieved from https://www.bleepingcomputer.com/news/security/microsoft-disrupts-onnx-phishing-as-a-service-infrastructure/

Gottfredson, M., & Hirschi, T. (2023). A General Theory of Crime in the Digital Age. *Cambridge University Press*.

Holt, T. J. (2023). Cybercrime as an Industry: The Evolution of Criminal Networks in the Digital Era. *Springer*.

Incibe. (2019, Agosto 07). *¿Sabías que las criptomonedas están involucradas en algunos ciberdelitos?* Retrieved from https://www.incibe.es/ciudadania/blog/sabias-que-las-criptomonedas-estan-involucradas-en-algunos-ciberdelitos

INCIBE. (2020, Enero 16). *Incibe*. Retrieved from Las 7 fases de un ciberataque. ¿Las conoces?: https://www.incibe.es/empresas/blog/las-7-fases-ciberataque-las-conoces

Interpol. (2023). Retrieved from Informe sobre Ciberdelincuencia 2023: https://www.interpol.int/es/Criminalidad/Ciberdelincuencia

Kaspersky. (2024). *Empresas de América Latina enfrentaron más de 268 millones de ataques en un año, según Kaspersky*. Retrieved from https://latam.kaspersky.com/about/press-releases/empresas-de-america-latina-enfrentaron-mas-de-268-millones-de-ataques-en-un-ano-segun-kaspersky

kaspersky. (2024, Octubre 22). *Grandoreiro, el troyano global con metas grandiosas.* Retrieved from https://securelist.lat/grandoreiro-banking-trojan/99206/

Kerner, S. M. (2025, Marzo 31). *Cybercrime-as-a-service explained: What you need to know*. Retrieved from https://www.techtarget.com/whatis/feature/Cybercrime-as-a-service-explained-What-you-need-to-know

Maimon, D., & Louderback, E. R. (2023). Cybercrime and Digital Forensics: The Social Science Perspective. *Oxford University Press*.

Miró Llinares, F. (2023). El cibercrimen en América Latina: Impacto y prevención. Lima: Fondo Editorial PUCP.

Moya, E., & Leticia, L. (2021). CRIME-AS-A-SERVICE: INTELIGENCIA COMPETITIVA EN EL LADO CIBERCRIMINAL PARA LA ERA POST-COVID19. *Journal of Economics & Business Intelligence*.

Newman, G., & Clarke, R. (2022). Rational Choice and Cybercrime: The Economics of Digital Offending. *Palgrave Macmillan.*

Omo-Ikerodah, L. (2024, marzo 4). *FaaS: What is it and why is Fraud-as-a-Service trending?* Retrieved from https://www.ravelin.com/blog/why-is-fraud-as-a-service-trending

Orbit. (2024, Diciembre 26). *Orbit*. Retrieved from CaaS: el cibercrimen como servicio y su impacto global: https://www.orbit.es/que-es-caas-el-cibercrimen-como-servicio/

Paesano, F. (2025, 02 10). *Cómo hacer frente a los delitos relacionados con las criptomonedas: Guía para las fuerzas de seguridad*. Retrieved from https://copolad.eu/es/delitos-criptomonedas/

Ponce M. (2024, 06 30). *Delitos informáticos: Caso Ecuador*. Retrieved from https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/2667/1665

Porras, R. (2023). Ciberdelincuencia en Ecuador: desafíos y perspectivas. *Tesisnet Internacional.*

Pujara, P. &. (2018). Phishing website detection using machine learning: a review. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 395-399.

Rudra, A. (2025, abril 25). *Malware como servicio (MaaS): ¿Qué es y cómo prevenirlo?* . Retrieved from https://powerdmarc.com/es/malware-as-a-service-maas/

Scotti, L. (2016). *Impacto de Internet en el mundo jurídico: Una mirada desde el Derecho Internacional Privado. Foro Jurídico.* Retrieved from https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/19845

Suler, J. (2024). The Online Disinhibition Effect. *CyberPsychology & Behavior*, pp. 321-326.

Sutherland, E. H., & Cressey, D. R. (2022). Criminología y Sociedad Digital: Perspectivas del Cibercrimen. *Buenos Aires: Ediciones Jurídicas del Sur*.

Taboada, P. S. (2019). ¿Por qué las organizaciones criminales utilizan criptomonedas? . *El Criminalista Digital. Papeles de Criminología*, 1-41.

Tal, C. (2024, Marzo 08). *Managing Cybersecurity Threats in Latin America*. Retrieved from https://infortal.com/managing-cybersecurity-threats-in-latin-america/

Tarlogic. (2023, Marzo 29). *Tarlogic*. Retrieved from Cyber Kill Chain. Diseccionar las 7 fases de un ciberataque dirigido: https://www.tarlogic.com/es/blog/cyber-kill-chain/

Technologies, A. (2025). *¿Qué es el ransomware BlackCat?* Retrieved from https://www.akamai.com/es/glossary/what-is-blackcat-ransomware

Trend Micro. (2024, 04 18). *The fall of LabHost: Law enforcement shuts down Phishing Service provider.* Retrieved from https://www.trendmicro.com/es_mx/research/24/d/labhost-takedown.html

Unir, M. (2021, 05 08). *Ciberdelincuencia: ¿qué es y cuáles son los ciberdelitos más comunes?* Retrieved from https://mexico.unir.net/noticias/ingenieria/que-es-ciberdelincuencia

Universo. (2024). *El Universo*. Retrieved from Ecuador es el tercer país con las mayores amenazas cibernéticas en América Latina, según Check Point: https://www.eluniverso.com/noticias/ecuador/ecuador-enfrenta-un-creciente-riesgo-de-ciberataques-en-el-2024-nota/

Vincent, B. (2018). *ASU, Arizona State University, Keep.* Retrieved from https://keep.lib.asu.edu/items/156823

Zuluaga, J. (2025, 4). *Cibercrimen como un Servicio: Un Negocio Menos Riesgoso y Más Rentable que el Narcotráfico*. Retrieved from https://www.linkedin.com/pulse/cibercrimen-como-un-servicio-negocio-menos-riesgoso-y-jaramillo-ejmte/

P.