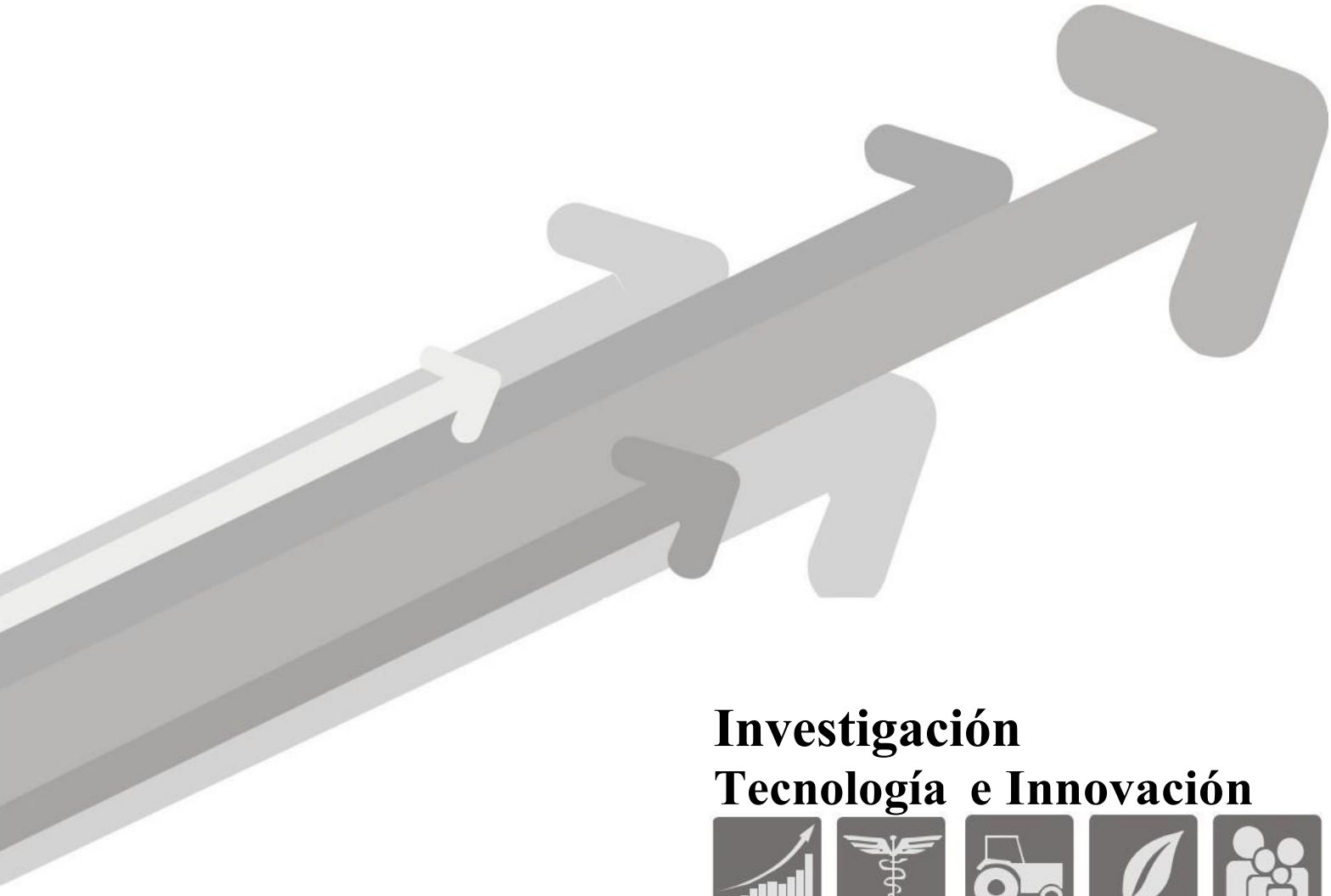
INVESTIGACIÓN, TECNOLOGÍA E INNOVACIÓN Vol. 17 No. 23 MAYO - 2025 (41-51)
ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

Elementos criminógenos de las tecnologías de la información y proliferación de la delincuencia informática

Criminogenic elements of information technologies and the proliferation of computer crime

Luis Mauricio Maldonado Ruiz



Investigación
Tecnología e Innovación

INVESTIGACIÓN, TECNOLOGÍA E INNOVACIÓN Vol. 17 No. 23 MAYO - 2025 (41-51)
ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

Elementos criminógenos de las tecnologías de la información y proliferación de la delincuencia informática

Criminogenic elements of information technologies and the proliferation of computer crime

Luis Mauricio Maldonado Ruiz[1]

Como citar: Maldonado Ruiz, L. M. (2025). Elementos criminógenos de las tecnologías de la información y proliferación de la delincuencia informática. *Investigación, Tecnología e Innovación*. 17(23), 41-51. DOI: https://doi.org/10.53591/iti.v17i23.1945

RESUMEN

Contexto: La era digital ofrece inmensas oportunidades gracias al uso de la tecnología, pero también plantea serios riesgos asociados a la facilitación de conductas criminales, conocidas en el ámbito jurídico como delitos informáticos o ciberdelitos. En el ámbito penal, este fenómeno ha generado un intenso debate sobre la capacidad de los tipos penales tradicionales para abordar las nuevas problemáticas derivadas del uso y abuso de los sistemas computacionales, agrupadas bajo el concepto de criminalidad informática. **Objetivo:** Analizar los delitos informáticos desde una perspectiva jurídico-penal, considerando su vinculación con la delincuencia transnacional y el crimen organizado, así como los desafíos que enfrentan los sistemas de justicia ante su creciente expansión. **Método:** Se empleó un enfoque cualitativo-descriptivo, sustentado en el análisis doctrinal y normativo de las legislaciones penales, así como en la revisión de estudios especializados sobre ciberdelincuencia y criminalidad organizada de carácter transnacional. **Resultados:** Se evidencia que los delitos informáticos han evolucionado rápidamente, superando las previsiones normativas tradicionales. Su carácter transfronterizo y su vínculo con redes delictivas organizadas dificultan su persecución penal efectiva, lo que contribuye en muchos casos a altos niveles de impunidad. **Conclusiones:** La lucha contra los delitos informáticos requiere una actualización normativa constante, cooperación internacional efectiva y un enfoque multidisciplinario que permita enfrentar la complejidad jurídica y tecnológica de estos delitos.

Palabras clave: Delitos informáticos, Ciberdelitos, Delincuencia transnacional, Crimen organizado, Impunidad.

ABSTRACT

Context: The digital era offers great opportunities through the use of technology, but it also poses serious risks related to the facilitation of criminal behaviors known in the legal field as computer crimes or cybercrimes. In criminal law, this phenomenon has raised intense debate about the adequacy of traditional legal frameworks to address new issues stemming from the misuse of digital systems, encompassed under the concept of cybercriminality. **Objective:** To analyze cybercrimes from a legal-criminal perspective, considering their connection with transnational crime and organized crime, and to examine the challenges faced by justice systems in the face of their increasing expansion. **Method:** A qualitative-descriptive approach was employed, based on doctrinal and legal analysis of criminal legislation, as well as a review of specialized studies on cybercrime and transnational organized crime. **Results:** The study shows that cybercrimes have evolved rapidly, surpassing the scope of traditional legal provisions. Their cross-border nature and link to organized criminal networks hinder effective criminal prosecution, often resulting in high levels of impunity. **Conclusions:** Combating cybercrime requires continuous legislative updates, effective international cooperation, and a multidisciplinary approach to address the legal and technological complexity of these offenses.

Keywords: Computer crimes, Cybercrimes, Transnational crime, Organized crime, Impunity

INVESTIGACIÓN, TECNOLOGÍA E INNOVACIÓN Vol. 17 No. 23 MAYO - 2025 (41-51)
ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

Fecha de recepción: diciembre 11, 2024.

Fecha de aceptación: mayo 20, 2025.

[1]Abogado y Master en Justicia Criminal y Criminología - Docente de la Universidad Internacional del Ecuador – UIDE.

INTRODUCCIÓN

El advenimiento de la tecnología informática ha dado lugar a un nuevo tipo de delito: el ciberdelito, que abarca diversas manifestaciones que implican el uso de ordenadores o redes informáticas. Ejemplos de ciberdelitos incluyen la propagación de virus informáticos, el fraude electrónico y la distribución de pornografía infantil a través de Internet.

A lo largo de la historia, la humanidad ha sido testigo de desarrollos dramáticos en todos los ámbitos, incluidas las tecnologías de la información y la comunicación, el mundo ha presenciado el surgimiento de nuevos tipos de delitos que no existían en siglos anteriores, a medida que todos los ámbitos de la vida se desarrollan de manera espectacular, también surgen nuevos métodos y formas de delito que evolucionan de manera peculiar, la presente investigación se centra en los delitos informáticos, también conocidos como delitos relacionados con la tecnología de la información o Internet, a pesar de los diferentes nombres, estos delitos tienen el mismo origen: el uso de Internet o las computadoras, esta investigación aborda la definición, las formas, los tipos y los métodos de los ciberdelitos, su ocurrencia, la manera de controlarlos, cómo rastrear a sus delincuentes, los sujetos del delito, los elementos esenciales de los mismos, así como la regulación e instrumentos internacionales existentes.

La revolución informática surgió como resultado de la sincronización de las tecnologías de la comunicación y la revolución de la información, este fenómeno, conocido en la actualidad como la "era de la información", representa un boom científico y tecnológico que estamos presenciando, la información ha sido, a lo largo de los siglos, la propiedad más valiosa del ser humano, y ha sido preservada y transmitida mediante diversas formas y medios, que han evolucionado gradualmente, esta evolución comenzó en los muros de templos y tumbas, pasó al papiro y culminó con la invención del papel, en la actualidad, la información se conserva en diversas formas, incluidas las tecnologías de almacenamiento electrónico, como los CD, DVD y memorias flash.

Los ciberdelitos se asemejan a los delitos tradicionales en cuanto a sus elementos: el autor, con motivos para cometer el delito; la víctima, que puede ser una persona física o jurídica; y las herramientas y el escenario del delito, in embargo, la principal diferencia entre ambos tipos de delitos radica en el uso de una herramienta tecnológica sofisticada en el ciberdelito, así como en el escenario donde se comete el crimen. En la mayoría de los casos, el ciberdelito se lleva a cabo de forma remota mediante redes y líneas de comunicación, entre el delincuente, la víctima y la ubicación geográfica desde donde se ejecuta el delito.

DESARROLLO.

Materiales y Métodos

La investigación analizó los elementos criminógenos de las tecnologías de la información y su relación con la proliferación de la delincuencia informática. Se basó en un enfoque cualitativo, descriptivo y exploratorio, utilizando fuentes secundarias como legislaciones nacionales e internacionales, estudios académicos, informes de organismos internacionales (ONU y OEA) y casos relevantes, como los de Kevin Mitnick, Julian Assange y el malware SpyEye. La revisión documental permitió identificar tendencias, tipologías y respuestas legales relacionadas con los ciberdelitos, contrastando normativas nacionales e internacionales y analizando trabajos doctrinales sobre criminología informática.

Para el análisis se categorizaron los ciberdelitos según su naturaleza, motivaciones y sujetos implicados. Se aplicó un enfoque deductivo para sintetizar hallazgos en categorías claras, destacando brechas normativas y mejores prácticas internacionales. El tratamiento de la información se llevó a cabo mediante revisión

ISSN: 1390-5147 / e-ISSN: 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

bibliográfica, estudio comparativo y análisis cualitativo de datos doctrinales y jurídicos. Este proceso aseguró un análisis riguroso y comprensivo de los factores que facilitan la proliferación de los ciberdelitos en el contexto de las TICs.

Ámbito de Definición de Delitos Informáticos.

Es complicado llegar a un consenso sobre una definición común de delito informático debido a las diversas interpretaciones derivadas del rápido avance de la tecnología de la información, por un lado, y la variabilidad en el papel que esta tecnología desempeña en la comisión de delitos, por otro. El sistema de información asociado a esta tecnología puede ser tanto el objetivo del delito como el medio utilizado para cometerlo. Si la investigación se centra en los delitos que afectan directamente al sistema de información, la definición se enfocará en la dimensión espacial, describiendo el delito como una acción dirigida contra dicho sistema. Por otro lado, si el análisis aborda los delitos perpetrados mediante el uso de tecnologías de la información, la definición girará en torno al medio: "Todas las formas de conducta ilícita realizadas a través del uso de computadoras" (BEQUAI, 2016, p. 145).

Cabe mencionar que uno de los factores más relevantes que dificulta un acuerdo sobre la definición de las tecnologías de la información (TI) es su capacidad para sustituir muchas tecnologías previas, como el teléfono, el fax y la televisión. Las TI no solo se limitan al procesamiento de datos, sino que también abarcan múltiples funciones, como la publicación y la copia, lo que hace indispensable diferenciar, desde una perspectiva técnica, entre los delitos cometidos a través de Internet y redes de información y aquellos. que utilizan Internet o computadoras como herramientas para llevarse a cabo.

Los delitos cibernéticos son aquellos que ocurren a través de Internet, redes de información o mediante el acceso no autorizado a redes privadas, como las de empresas, bancos y otras entidades. Incluyen el uso indebido de datos digitales que contienen información, tales como falsificación, corrupción, eliminación de datos, o posesión ilegal de herramientas o secretos. En estos casos, la tecnología de la información juega un papel fundamental, ya sea como elemento material del delito o como facilitador de la conducta delictiva.

Por otro lado, existen delitos tradicionales, como el lavado de dinero, el narcotráfico, el terrorismo, la prostitución, el uso ilícito de tarjetas electrónicas, la pornografía o delitos relacionados con el comercio electrónico, así como los de calumnia y difamación que utilizan. las tecnologías de la información como herramienta para llevarse a cabo. Sin embargo, estos no siempre se consideran ciberdelitos desde un punto de vista técnico, aunque a menudo se les denomina como cuentos.

La Naturaleza y las Formas de los Delitos Informáticos

El cibercrimen comprende un amplio espectro de actividades ilegales realizadas mediante dispositivos electrónicos y redes digitales. Estos delitos pueden clasificarse según la naturaleza de su impacto, el rol de la tecnología y los efectos en las víctimas.

Clasificación según la naturaleza del delito

1. Delitos contra los sistemas informáticos: incluyen sabotaje, ataques de denegación de servicio (DoS) y la instalación de malware.
2. Delitos contra datos personales: abarcan el robo de identidad, la falsificación de información y el acceso no autorizado.
3. Delitos contra la propiedad intelectual: como la piratería de software y la distribución ilegal de contenido protegido (Sieber, 1992).

Clasificación según el rol de la tecnología

- Tecnología como objetivo: los sistemas son el blanco principal, como en casos de sabotaje o eliminación de datos.

INVESTIGACIÓN, TECNOLOGÍA E INNOVACIÓN Vol. 17 No. 23 MAYO - 2025 (41-51)
ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

- Tecnología como herramienta: la tecnología se utiliza para cometer fraudes, estafas o difundir contenido ilícito.

Clasificación según el impacto en las víctimas

- Ataques a la privacidad: incluyen el acoso cibernético y la divulgación no autorizada de información.
- Delitos económicos: abarcan fraudes financieros, phishing y robo de fondos digitales.
- Delitos contra la seguridad estatal: como el ciberterrorismo y el espionaje industrial.

La velocidad con la que se desarrollan nuevas tecnologías amplifica tanto los beneficios como los riesgos asociados. Los ciberdelitos no solo afectan a individuos, sino también a corporaciones e incluso a gobiernos, como lo demuestran los numerosos ataques a infraestructuras críticas reportados en la última década (UNODC, 2013).

Sujetos del Delito

La historia demuestra que los delitos informáticos son cometidos por una amplia gama de personas: estudiantes, aficionados, terroristas y miembros de grupos del crimen organizado. Lo que los distingue es la naturaleza específica del delito. Por ejemplo, una persona que accede a un sistema informático sin intención delictiva significativa es muy distinta de un empleado de una institución financiera que sustrae fondos de las cuentas de los clientes.

El nivel de habilidad del delincuente informático es un tema controvertido. Mientras algunos sostienen que la habilidad técnica no es un factor determinante, otros afirman que los posibles delincuentes informáticos suelen ser individuos brillantes, motivados y dispuestos a aceptar desafíos tecnológicos. Paradójicamente, estas características también son valoradas en el ámbito profesional del procesamiento de datos.

El comportamiento delictivo relacionado con la informática abarca un amplio espectro de la sociedad. Los delincuentes informáticos tienen edades que van desde los 10 hasta los 60 años y niveles de habilidad que oscilan entre principiantes y profesionales. Por ello, estos delincuentes no necesariamente son “súper-criminales" con talentos únicos, sino personas promedio que, con un mínimo de conocimiento técnico, pueden convertirse en potenciales perpetradores. Las motivaciones pueden ser tan diversas como el desafío tecnológico, el deseo de ganancia económica, la búsqueda de notoriedad, la venganza o la promoción de ideologías.

Es pertinente definir el delito informático como todo acto delictivo que involucra una o más computadoras, ya sea como objetivo del delito o como herramienta para su comisión. Estos delitos pueden subdividirse en dos categorías:

1. **Crímenes relacionados con la informática**: La computadora o su contenido son el objetivo principal del delito, como en casos de piratería o ataques de denegación de servicio.
2. **Delitos asistidos por computadora**: La computadora se utiliza como herramienta para cometer delitos que, en principio, podrían ejecutarse por otros medios, como el fraude financiero o la malversación de fondos (ACURIO DEL PINO, 2010).

Existe una falsa creencia de que los autores de delitos informáticos son siempre especialistas en tecnologías. Aunque un conocimiento básico es necesario, no implica que deban ser profesionales en el área. Los delincuentes informáticos son tan variados como los delitos que cometen. En el caso de los delitos financieros, como el fraude o el robo de información, la mayor parte es atribuible a empleados de empresas, responsables del 90% de estos casos según el *Manual de las Naciones Unidas de 1997 sobre la prevención y fiscalización de los delitos relacionados con las computadoras*.

INVESTIGACIÓN, TECNOLOGÍA E INNOVACIÓN Vol. 17 No. 23 MAYO - 2025 (41-51)
ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

Por ejemplo, el Servicio Secreto de los Estados Unidos estima que los consumidores pierden aproximadamente 500 millones de dólares anuales debido al robo de números de tarjetas de crédito y llamadas en línea. Estos datos son vendidos por sumas considerables a falsificadores, quienes utilizan programas especializados para codificarlos en las bandas magnéticas de tarjetas bancarias y de crédito, según señala el Manual de la ONU.

Perfiles de los sujetos activos

1. Hackers: buscan vulnerabilidades en sistemas como desafío técnico, a menudo sin intención directa de causar daño.
2. Crackers: violan sistemas de seguridad con fines destructivos, lucrativos o de notoriedad.
3. Insiders: empleados que abusan de su acceso privilegiado para robar información, cometer fraudes o sabotear operaciones.
4. Newbies: usuarios con habilidades limitadas que utilizan herramientas automatizadas para realizar actividades ilícitas.

Motivaciones de los sujetos activos

Según el Manual de la ONU (1997), la mayoría de los delitos informáticos tienen motivaciones económicas, aunque también pueden incluir razones personales, ideológicas o técnicas. Un ejemplo notable es el espionaje industrial, donde los empleados sustraen información para venderla a competidores.

Los avances tecnológicos y la disponibilidad de herramientas automatizadas han reducido las barreras para entrar en el mundo del ciberdelito, permitiendo que individuos con conocimientos limitados puedan participar en actividades ilícitas. Esto ha llevado a un aumento exponencial en la cantidad de ataques reportados anualmente (Bequai, 2016).

Motivaciones del Ciberdelincuente

El sujeto activo de un delito informático puede estar impulsado por una gran variedad de motivaciones, lo que hace difícil descifrar su verdadera intención. Mientras que algunos violan la seguridad de los sistemas informáticos por mera curiosidad, otros buscan objetivos más específicos como multas económicas, reconocimiento personal o venganza. En muchos casos, estos individuos desean satisfacer una necesidad interna de poder o demostrar su superioridad intelectual. Sin embargo, estas motivaciones pueden estar influenciadas tanto por factores internos como externos, como el deseo de mostrar habilidades excepcionales, enviar un mensaje ideológico o, incluso, realizar acciones que perciben como beneficiosas para el colectivo.

Según FIGOLI (1998), citado por ACURIO (2015, p. 86), las principales motivaciones de los delincuentes informáticos, denominados *hackers* o *crackers*, se clasifican en las siguientes categorías:

1. **Motivación Social:** El objetivo es obtener la aceptación y el reconocimiento de sus pares. En el mundo del hacking, la competitividad otorga estatus y posicionamiento dentro de la jerarquía social del grupo.
2. **Motivación Técnica:** En este caso, el propósito es exponer las vulnerabilidades de un sistema, lo que no solo demuestra el conocimiento técnico del atacante, sino que también obliga a la industria a perfeccionar la seguridad y la integridad de sus operaciones.
3. **Motivación Política:** Está relacionada con la promoción de ideologías políticas mediante el uso de herramientas informáticas para influir en la opinión pública o desestabilizar a los gobiernos.

INVESTIGACIÓN, TECNOLOGÍA E INNOVACIÓN Vol. 17 No. 23 MAYO - 2025 (41-51)
ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

4. **Motivación Económica:** Incluye conductas ilícitas como el fraude o el espionaje empresarial, particularmente entre empresas competidoras, donde la obtención de ventajas económicas es el principal incentivo.

5. **Motivación Laboral**: Algunos aspirantes a puestos relacionados con sistemas informáticos intentan demostrar su capacidad técnica poniendo a prueba las seguridades de los sistemas de una empresa, o incluso sugiriendo mejoras como una forma de destacar sus aptitudes.

6. **Motivación Gubernamental**: Algunas acciones son impulsadas por intereses de los Estados, que buscan ventajas estratégicas mediante el espionaje o la ciberguerra, con el propósito de obtener información sensible o debilitar a naciones adversarias.

Estas motivaciones, aunque no abarcan todas las posibles, son las más notables según Figoli. Los delincuentes informáticos pueden ser desde simples ladrones de información, motivados por beneficios económicos, hasta individuos que buscan generar repercusiones sociales significativas. Un ejemplo de esta última categoría es quienes padecen el llamado "Síndrome de Robin Hood", justificando sus acciones ilícitas bajo la idea de que están contribuyendo a hacer del mundo un lugar mejor. Sin embargo, aunque sus motivaciones puedan parecer justas, las consecuencias de sus actos suelen vulnerar los derechos de muchas personas.

Por su parte, ROGERS (1999), citado por ARROYO (2020, p. 111), en su obra *Un enfoque bidimensional para el desarrollo de una taxonomía de piratas informáticos*, clasifica las motivaciones de los delincuentes informáticos según sus capacidades técnicas:

- **El Novato**: Un principio que utiliza herramientas automáticas y busca hacerse un nombre en el ámbito del hacking.
- **El Ciberpunk**: Con conocimientos básicos de programación, este tipo de delincuente busca fama y beneficios económicos.
- **El Iniciado**: Ataca desde dentro de su lugar de trabajo como forma de venganza contra su empleador.
- **El Simple Ladrón**: Traslada su actividad delictiva del mundo físico al virtual, atacando principalmente bancos y empresas de tarjetas de crédito con multas económicas.
- **El Pirata de la Vieja Escuela**: Motivado por el desafío intelectual, mantiene la mentalidad de los hackers tradicionales.
- **El Criminal Profesional**: Especializado en delitos informáticos, busca beneficios económicos significativos.
- **El Guerrero de la Información**: Su objetivo es desestabilizar centros de toma de decisiones, ya sea por razones ideológicas o estratégicas.

INVESTIGACIÓN, TECNOLOGÍA E INNOVACIÓN Vol. 17 No. 23 MAYO - 2025 (41-51)
ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

La clasificación de Rogers ofrece un enfoque interesante al relacionar las motivaciones con los distintos perfiles de delincuentes informáticos. Aunque puede considerarse una tipología híbrida, su perspectiva refleja la realidad de la diversidad de estos actores.

En general, las motivaciones del sujeto activo en los delitos informáticos son variadas y están vinculadas con el tipo de ilícito cometido. Por ejemplo, el fraude informático suele estar impulsado por el lucro económico, mientras que el sabotaje tiende a ser motivado por la venganza o el resentimiento personal. Otros delitos, como los relacionados con el terrorismo cibernético o la ciberguerra, tienen raíces ideológicas o políticas.

En definitiva, no es posible establecer un patrón único para las motivaciones de los delincuentes informáticos. Cada infractor se mueve por sus propias creencias, necesidades o aspiraciones, lo que refleja la complejidad del fenómeno.

Tipología Común de los Delitos Informáticos

Los delitos informáticos han surgido como una de las mayores preocupaciones en la sociedad contemporánea debido a la proliferación de tecnologías digitales y la expansión de Internet. Estos delitos, facilitados por las redes globales y las plataformas en línea, abarcan una amplia variedad de conductas delictivas, cada una con características y motivaciones particulares. Para comprender mejor este fenómeno, podemos agrupar los delitos informáticos en tres grandes categorías, que reflejan su diversidad y complejidad:

1. Delitos con la computadora como objetivo

Esta categoría se refiere a delitos cuyo objetivo principal es dañar, alterar o sabotear los sistemas informáticos y las redes digitales en sí mismas. Estos delitos pueden tener consecuencias devastadoras tanto para las personas como para las empresas, afectando la integridad, disponibilidad y confidencialidad de los sistemas. Los infractores, en este caso, se centran en la tecnología como su blanco. Los principales tipos incluyen:

- **Ataques de Denegación de Servicio (DoS):** Estos ataques buscan sobrecargar un servidor o red con un volumen excesivo de tráfico, de modo que el sistema objetivo se ve incapaz de manejar todas las solicitudes y, por lo tanto, queda fuera de servicio. Este tipo de ataques puede paralizar sitios web de gran envergadura, provocando pérdidas económicas significativas y afectando la confianza del usuario.

- **Instalación de Malware:** El malware incluye virus, troyanos, ransomware, spyware y otros programas maliciosos que pueden ser utilizados para robar información, espiar a los usuarios o incluso tomar el control de los dispositivos infectados. Estos ataques pueden propagarse rápidamente y comprometer grandes redes de computadoras, tanto personales como corporativas. Además, los ciberdelincuentes pueden utilizar el malware para crear botnets (redes de computadoras infectadas) que realizan ataques masivos de denegación de servicio (DDoS) o roban información valiosa.

- **Sabotaje Informático:** Este delito implica la alteración maliciosa o destrucción de datos críticos, interrumpiendo las operaciones de una empresa o institución. Un ejemplo de sabotaje es la destrucción de bases de datos que contienen información valiosa o las alteraciones de códigos de software que impiden que los sistemas funcionen correctamente. Los ataques de sabotaje también pueden incluir las alteraciones de registros financieros o datos científicos, con el propósito de causar daño a las organizaciones afectadas.

INVESTIGACIÓN, TECNOLOGÍA E INNOVACIÓN Vol. 17 No. 23 MAYO - 2025 (41-51)
ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

2. Delitos tradicionales cometidos mediante computadoras

Las tecnologías digitales no solo han permitido la creación de nuevos tipos de delitos, sino que también han facilitado la ejecución de delitos tradicionales de manera más eficiente. A través de internet y las plataformas digitales, los delincuentes pueden acceder a un gran número de víctimas con facilidad. Algunos ejemplos de delitos tradicionales cometidos mediante el uso de computadoras incluyen:

- **Fraude Financiero:** El fraude en línea es uno de los delitos más comunes en la era digital. Los delincuentes utilizan plataformas de comercio electrónico, correos electrónicos fraudulentos (phishing), y sitios web falsificados para engañar a las personas y obtener información financiera como números de tarjetas de crédito o datos bancarios. Con esta información, los delincuentes pueden realizar compras no autorizadas, transferir dinero o incluso crear identidades falsas.

- **Robo de Identidad:** En el contexto digital, el robo de identidad se ha convertido en un problema creciente. Los ciberdelincuentes obtienen datos personales como nombres, direcciones, números de seguridad social, detalles de cuentas bancarias, entre otros, con el fin de suplantar la identidad de una persona. Esto les permite abrir cuentas bancarias fraudulentas, solicitar tarjetas de crédito, o incluso realizar acciones ilegales en nombre de la víctima, lo que genera perjuicios económicos y emocionales a las personas afectadas.

- **Falsificación de Documentos Electrónicos:** Con la digitalización de documentos legales y administrativos, los delincuentes han aprovechado las vulnerabilidades de los sistemas para falsificar documentos como contratos, certificados, pasaportes, facturas electrónicas, entre otros. Estos documentos pueden ser utilizados para cometer fraudes, eludir regulaciones legales o facilitar otros delitos como el lavado de dinero.

3. Computadoras como repositorios de evidencia

En esta categoría, la computadora no es el objeto del delito en sí, sino que se utiliza como un medio para almacenar o distribuir información ilegal. Los ciberdelincuentes utilizan dispositivos electrónicos para guardar evidencia de actividades ilícitas, que luego pueden ser utilizados para investigaciones criminales o el esclarecimiento de delitos. Algunos ejemplos de este tipo de delitos incluyen:

- **Pornografía infantil:** Aunque los delitos de explotación infantil no son nuevos, la digitalización y la facilidad para compartir archivos en línea han incrementado la magnitud del problema. Las computadoras se utilizan para almacenar y distribuir material ilegal como imágenes y videos de abuso infantil. A través de redes sociales, foros ocultos o plataformas de intercambio de archivos, los delincuentes pueden distribuir dicho contenido a nivel mundial, lo que hace difícil su detección y persecución.

- **Registros Financieros Ilícitos:** Muchas actividades delictivas, como el lavado de dinero o la evasión fiscal, se facilitan mediante el uso de computadoras y sistemas electrónicos. Los delincuentes crean registros financieros falsificados, realizan transferencias ilegales o mantienen bases de datos ocultas

ISSN: 1390-5147 / e-ISSN: 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

para encubrir sus actividades delictivas. Estos registros pueden ser almacenados en dispositivos de almacenamiento externos o en la nube, lo que complica la labor de las autoridades para rastrear el dinero ilegal.

Regulación Internacional de la Delincuencia Informática

El carácter transnacional de los delitos informáticos hace que la cooperación internacional y los marcos legales armonizados sean cruciales para su prevención y persecución. Sin embargo, las disparidades en las legislaciones nacionales dificultan este proceso, dejando vacíos legales que los ciberdelincuentes pueden explotar. A continuación, se detallan algunas de las iniciativas internacionales más relevantes para enfrentar el cibercrimen:

1. Convenio de Cibercriminalidad del Consejo de Europa

Adoptado en 2001, el **Convenio de Cibercriminalidad,** también conocido como la **Convención de Budapest**, establece estándares comunes entre los países firmantes para la lucha contra los delitos informáticos. Este tratado abarca una amplia gama de delitos, incluyendo el acceso ilegal a sistemas informáticos, la interferencia con datos, la falsificación de documentos electrónicos y el fraude informático. Además, promueve la cooperación entre los países miembros en la investigación y persecución de los delincuentes informáticos, estableciendo mecanismos para el intercambio de información, la asistencia mutua y la armonización de las leyes nacionales.

2. Iniciativas de la ONU

La **Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)** ha sido un actor clave en la creación de marcos legales y programas de cooperación internacional en el ámbito de la ciberseguridad. A través de la capacitación, la asistencia técnica y el fomento de buenas prácticas, la ONU trabaja para mejorar la capacidad de los países para abordar los delitos informáticos y proteger la infraestructura crítica. También fomenta la cooperación internacional en investigaciones transnacionales, ayudando a los países a abordar la ciberdelincuencia de manera coordinada.

3. Estrategias de la OEA

La **Organización de Estados Americanos (OEA)** ha implementado varias estrategias y programas de ciberseguridad en América Latina y el Caribe, con el fin de fortalecer la resiliencia de los Estados frente a las amenazas cibernéticas. La OEA trabaja en la creación de marcos legales nacionales que abordan la ciberdelincuencia, proporciona capacitación a personal técnico y fomenta el intercambio de información y experiencias entre países. Además, se enfoca en mejorar la protección de infraestructuras críticas y en promover una cultura de ciberseguridad en la región.

La cooperación internacional es, por tanto, un pilar esencial para enfrentar la creciente amenaza de la ciberdelincuencia. La rápida evolución de las tecnologías digitales requiere una respuesta ágil y flexible por parte de los gobiernos y las organizaciones internacionales, lo que implica una actualización constante de las normativas, las estrategias de ciberseguridad y las capacidades de investigación de los Estados. Solo a través de un enfoque global y coordinado será posible abordar los retos de la delincuencia informática en el futuro.

CONCLUSIONES

El fenómeno de la delincuencia informática es un tema complejo debido a las características particulares de los sujetos que cometen estos delitos. Como se analizó en esta investigación, el sujeto activo de la delincuencia informática posee conocimientos técnicos avanzados y habilidades en el uso de tecnologías de la información, lo que le permite manipular datos, destruir redes, falsificar tarjetas electrónicas y modificar bases de datos, lo que da lugar a diversos tipos de delitos informáticos. Las víctimas de estos delitos pueden estar dispersas en

ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

todo el mundo, dado que el delito informático trasciende las fronteras nacionales, lo que plantea la necesidad de una armonización normativa a través de acuerdos y tratados internacionales para abordar eficazmente la criminalidad informática.

La naturaleza y las formas de los delitos informáticos presentan desafíos adicionales en términos de enjuiciamiento y detección. La omnipresencia de estos delitos dificulta la identificación del perpetrador, lo que complica la asignación de responsabilidad penal y la reparación de los daños sufridos por las víctimas. La capacidad de los delincuentes para difundir contenido a través de dispositivos como teléfonos móviles hace aún más difícil para los gobiernos restringir estas actividades delictivas. Además, muchos ciberdelincuentes no pueden ser identificados antes de cometer el delito, lo que obliga a las empresas a centrarse en medidas preventivas para frenar diversas actividades delictivas.

En cuanto a las motivaciones de los ciberdelincuentes, se destacan diferencias individuales, como rasgos de personalidad y el contexto en línea. Las motivaciones varían, siendo las ganancias financieras la principal razón para muchos delitos cibernéticos, como el phishing, fraudes en línea y el malware. Sin embargo, otros ciberdelincuentes actúan por razones como el activismo, el espionaje, el robo cibernético o incluso como una broma.

Respecto a los tipos de delitos informáticos, podemos observar que en algunos casos el dispositivo informático es el objetivo del delito, como en los ataques para obtener acceso no autorizado a redes. En otros, la computadora se utiliza como arma, como en los ataques de denegación de servicio (DoS). También existen delitos en los que la computadora actúa como cómplice, como en los casos donde se almacena información obtenida ilegalmente.

Finalmente, la investigación sobre la criminalidad informática debería continuar explorando la seguridad informática en sociedades y democracias emergentes, con el fin de mejorar la normativa y las capacidades técnicas de sus sistemas. Además, es esencial analizar la aplicación de los convenios y tratados internacionales en los sistemas jurídicos de los países firmantes para evaluar la efectividad de las directrices en el tratamiento de los delitos cibernéticos.

AGRADECIMIENTOS

El presente artículo ha sido posible gracias al espacio académico otorgado por la Universidad Internacional del Ecuador (UIDE), institución en la que desempeño labores como docente e investigador, permitiéndome desarrollar y profundizar en el ámbito de la investigación científica. Extiendo mi más sincero reconocimiento a mi familia, cuyo respaldo incondicional, paciencia y motivación constante han sido esenciales para la concreción de este trabajo, sirviendo de inspiración en cada etapa del proceso.

REFERENCIAS BIBLIOGRÁFICAS

Acurio del Pino. (2010). Informática jurídica y derecho informático. Quito, Ecuador: Universidad Central Editor.

Acurio del Pino. (2015). Derecho informático (1.ª ed., p. 86). Quito, Ecuador: Universidad Central Editor. ISBN 9789942081156

Arroyo, J. (2020). Un enfoque bidimensional para el desarrollo de una taxonomía de piratas informáticos (p. 111). Quito, Ecuador: Fondo Editorial de la Universidad Central.

Bequai, A. (2016). "El sujeto activo de la delincuencia informática posee conocimientos técnicos avanzados y habilidades en el uso de tecnologías de la información, lo que le permite manipular datos, destruir redes, falsificar tarjetas electrónicas y modificar bases de datos, lo que da lugar a diversos tipos de delitos informáticos" (Bequai, 2016, p. 102).

ISSN: 1390-5147 / **e-ISSN:** 2661-6548
DOI: https://doi.org/10.53591/iti.v17i23.1945

Bequai, A. (2016). *Cybercrime and security* (Rev. ed.). Nueva York, NY: Praeger. ISBN 9780275927574

Consejo de Europa. (2001). "El carácter transnacional de los delitos informáticos exige respuestas jurídicas coordinadas entre países, pues los marcos legales tradicionales no son suficientes para enfrentar el fenómeno" (Consejo de Europa, 2001).

Consejo de Europa. (2001). "El uso de convenios internacionales es clave para el abordaje de la criminalidad informática, promoviendo la cooperación internacional y la implementación de normativas comunes para enfrentar este fenómeno" (Consejo de Europa, 2001, p. 24).

OEA. (2012). Estrategia interamericana de ciberseguridad. Washington, D.C.: OEA. Recuperado de https://www.oas.org/es/ciberseguridad/

ONU. (1997). Manual sobre el uso de tecnologías de la información en la delincuencia organizada transnacional. Viena, Austria: Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC).

Sieber, U. (1992). "La naturaleza y las formas de los delitos informáticos presentan desafíos adicionales en términos de enjuiciamiento y detección. La omnipresencia de estos delitos dificulta la identificación del perpetrador" (Sieber, 1992, p. 58).

Sieber, U. (1992). The threat of cybercrime: Problems and solutions in international law. Oxford, England: Clarendon Press. ISBN 9780198256655

UNODC. (2013). *Estudio integral sobre la delincuencia organizada transnacional y las nuevas tecnologías*. Viena, Austria: Naciones Unidas. Recuperado de https://www.unodc.org/documents/organized-crime/UNODC_Informe_Tecnologia_2013.pdf

UNODC. (2013). "Las motivaciones de los ciberdelincuentes varían, siendo las ganancias financieras la principal razón para muchos delitos cibernéticos, como el phishing, fraudes en línea y el malware" (UNODC, 2013, p. 89).