UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

ESCUELA DE CIENCIAS JURÍDICAS

UNIDAD DE POST GRADO

MAESTRÍA EN DERECHO PENAL ECONÓMICO

ANÁLISIS DEL DELITO DE ESTAFA INFORMATICA EN LA COMERCIALIZACION DE CRIPTOACTIVOS EN EL SALVADOR

TESIS PARA OBTENER EL GRADO DE:

MAESTRA EN DERECHO PENAL ECONÓMICO

PRESENTADO POR:

SONIA JUDITH PEÑA CALDERON

ASESOR DE CONTENIDO:

DOCTOR. ARMANDO ANTONIO SERRANO

CIUDAD UNIVERSITARIA, SAN SALVADOR, JUNIO 2025.

AUTORIDADES UNIVERSIDAD DE EL SALVADOR

Ing. Juan Rosa Quintanilla
RECTOR

Dra. Evelin Beatriz Farfán Mata
VICERRECTOR ACADEMICO

MSc. Roger Armando Arias Alvarado
VICERRECTOR ADMINISTRATIVO

Lic. Pedro Rosalío Escobar Castaneda
SECRETARIO GENERAL

AUTORIDADES
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

MSc. Hugo Dagoberto Pineda Argueta
DECANO

MSc. Oscar Mauricio Duarte Granados
VICEDECANO

Dr. José Humberto Morales
DIRECTOR DE UNIDAD DE ESTUDIOS DE POSGRADO

DEDICATORIA

A Dios todopoderoso por permitirme alcanzar un logro más de su mano

A mi familia y en especial a mi mamá y a mi querida Daniela por esta conmigo y apoyarme, por ser mi inspiración.

A mi asesor de tesis por la confianza y la motivación en este proyecto hasta lograrlo.

"Andábamos sin buscarnos, pero sabiendo

que andábamos para encontrarnos"

— Julio Cortázar

"A ti, que fuiste el primer lector de cada página de este trabajo.

Existen personas que sin saberlo son en esencia, el motor silencioso detrás de todo logro e inspiración.

Creíste en esta investigación con una convicción que muchas veces superó a la mía propia. Tu inteligencia tocó estas ideas, tu paciencia sostuvo este proceso y tu fe en mí fue, sin duda, el fundamento más sólido sobre el que se construyó esta tesis.

Hay mentes que nos desafían, nos inspiran a ser mejores, nos moldean, en las que confiamos y creemos porque su autenticidad es su marca personal.

Fuiste, en el sentido más profundo de la palabra, parte de esta obra."

CONTENIDO

INTRODUCCIÓN

El vertiginoso avance de la tecnología ha transformado cada faceta de la vida contemporánea, abriendo nuevas fronteras para el comercio, la comunicación y las finanzas. En este escenario de digitalización global, la emergencia de los criptoactivos, como Bitcoin y Ethereum, representa una de las innovaciones financieras más disruptivas de las últimas décadas. Su naturaleza descentralizada, su promesa de transparencia y su potencial para democratizar el acceso a los servicios financieros han captado la atención de millones de personas e instituciones en todo el mundo. Sin embargo, esta misma promesa de disrupción, unida a la complejidad técnica, la volatilidad inherente y la relativa novedad de su marco regulatorio, ha creado un terreno fértil para nuevas y sofisticadas formas de criminalidad.

El Salvador, inmerso en este paradigma con la adopción hace unos años del Bitcoin como moneda de curso legal (pese a que a la fecha ya no es así), se encuentra en una posición única en el mapa global de las criptodivisas. Esta vanguardia tecnológica, si bien trae consigo oportunidades sin precedentes para la inclusión financiera y el desarrollo económico, también expone al sistema jurídico salvadoreño a desafíos complejos en la persecución de delitos emergentes. Entre estos, el delito de estafa informática se erige como una de las amenazas más persistentes y dañinas en el ámbito de la comercialización de criptoactivos.

Los criminales, cada vez más sofisticados y apoyados en herramientas de inteligencia artificial (IA), explotan las brechas de conocimiento, la inexperiencia de los inversores y las debilidades en los sistemas de seguridad para perpetrar fraudes masivos, que van desde esquemas Ponzi disfrazados de "oportunidades cripto" hasta la suplantación de identidad avanzada y el uso de plataformas falsas.

La presente tesis para optar al grado de maestra en Derecho Penal Económico aborda la intrincada relación entre la estafa informática y la comercialización de Criptoactivos en El Salvador. Su objetivo principal es analizar de manera crítica la tipificación del delito de estafa informática en la legislación salvadoreña, particularmente bajo la Ley Especial Contra los Delitos Informáticos y Conexos (LEDIC), y evaluar su idoneidad y capacidad de respuesta frente a las modalidades delictivas que surgen en este ecosistema financiero descentralizado.

En el capítulo uno se desarrollaran los conceptos claves que son necesarios para comprender la tipología de los delitos informáticos en su aspecto técnico y especialmente el delito de estafa informática, desarrollaremos aspectos vinculados a la informática, las tecnologías de la información y comunicación y el funcionamiento de la red de redes "la internet", esto con el objeto de comprender la infraestructura tecnológica a la que nos enfrentamos a la hora de investigar el delito de estafa informática.

El capítulo dos ofrecerá una visión general de los criptoactivos centrándose en sus aspectos fundamentales y cómo se compra vende y utilizan, se explicara el surgimiento de las criptomonedas seguido de cuestiones técnicas en las que se desarrollaran conceptos fundamentales para comprender la comercialización de los mismos y se profundizará en la relación crucial entre criptografía y blockchain y asimismo en el proceso de creación de billeteras, para finalmente abordar las consideraciones importantes relacionadas con el comercio de Criptoactivos incluyendo alertas relacionadas a su comercialización, el concepto de debida diligencia en este contexto y el entorno regulatorio de los mismos.

El análisis legal exhaustivo de la estafa informática desde su naturaleza fundamental y definición hacia los elementos específicos de este tipo penal corresponde al tercer capítulo de esta tesis,

requeridos para constituir el delito, asimismo se profundizará en los métodos contemporáneos a través de los cuales se ejecuta la acción típica requerida es decir las metodologías vinculadas al uso de tecnologías de la información y comunicación.

Se explorarán las particularidades de la causalidad lógica y la imputación objetiva en el contexto de una estafa informática donde la interacción humana puede ser mínima o mediada por sistemas automatizados y la IA.

En el capítulo cuatro se examinará el papel fundamental de la evidencia digital y haciendo especial énfasis en el rol y la eficacia de herramientas de investigación como el agente digital encubierto, considerando los desafíos que impone la naturaleza transfronteriza y pseudónima de las transacciones con criptoactivos.

Finalmente, en el capítulo cinco, se propondrán lineamientos para el fortalecimiento del marco jurídico-penal y la capacidad institucional del Estado salvadoreño para combatir eficazmente esta forma de delincuencia económica a través de la conclusiones y recomendaciones.

.

ABREVIATURAS

Art.	**Artículo**
AML	**Anti-lavado de Dinero**
CATV	**Redes de televisión por cable**
CDPC	**Comité Europeo para los problemas Criminales**
CP	**Código Penal**
CPP	**Código Procesal Penal**
CSJ	**Corte Suprema de Justicia**
DLT	**Tecnología de Registro Distribuido**
DNS	**Sistema de Nombres de Dominio**
FGR	**Fiscalía General de la Republica**
GAFI	**Grupo de Acción Financiera**
IP	**Internet Protocol**
ISO	**International Organization for Standardization**
ISP	**Proveedor de servicios de Internet**
KYC	**Conoce a tu Cliente**
LADs	**Link Access devices**
LAN	**Local Área Network**
LDA/FT/FPADM	**Lavado de Dinero y Activos, Financiamiento al terrorismo y la Proliferación de Armas de Destrucción Masiva**
LEAD	**Ley de Emisión de Activos Digitales**
LEDIC	**Ley Especial contra Delitos Informáticos y Conexos**
M.A.N.	**Redes de Área Metropolitana**
NFT	**Non-Fungible Token**

OCDE	**Organización de Cooperación y Desarrollo Económico**
PNC	**Policía Nacional Civil**
RFC	**Request for Comments**
TI	**Tecnología de la Información**
TIC	**Tecnología de la información y Comunicación**
UIF	**Unidad de Investigación Financiera**
VASPs	**Proveedor de Servicios de Activos Virtuales**
VPN	**Redes Privadas Virtuales**
WAN	**Redes de Área Extensa**

ANÁLISIS DEL DELITO DE ESTAFA INFORMATICA EN LA COMERCIALIZACION DE CRIPTOACTIVOS EN EL SALVADOR

POR

Sonia Judith Peña Calderón

RESUMEN

Esta investigación surge de la necesidad de comprender cómo la delincuencia económica ha encontrado en el ciberespacio un terreno fértil para evolucionar, enfocándose específicamente en cómo se configura el delito de estafa informática dentro del mercado de los Criptoactivos en El Salvador. El punto de partida es claro: hoy en día, el derecho penal económico no puede aplicarse a ciegas de la tecnología. Comprender el funcionamiento de Internet, las TIC y la informática no es un asunto secundario, sino el único camino para entender la migración de los delitos tradicionales hacia plataformas automatizadas y entornos que ya utilizan Inteligencia Artificial. Por ello, en sintonía con marcos internacionales como el Convenio de Budapest, esta tesis asume que la solución no es crear un derecho penal aislado para el entorno digital, sino integrar y adaptar nuestras categorías jurídicas tradicionales a los retos que plantean la criptografía y la tecnología *blockchain*.

Al aterrizar este fenómeno en la realidad salvadoreña [marcada por la audaz adopción de la *Ley Bitcoin* en 2021 y la posterior *Ley de Emisión de Activos Digitales (LEAD)*], la investigación se adentra en el análisis crítico del artículo 10 de la Ley Especial contra los Delitos Informáticos y Conexos (LEDIC). Desde una perspectiva dogmática, sostengo que la estafa informática es un delito pluriofensivo que va más allá del simple daño patrimonial; afecta también, de forma directa, la seguridad de los sistemas que procesan datos de manera automatizada.

El núcleo del debate teórico que propongo se centra en marcar una frontera clara entre la estafa tradicional y la informática. En la modalidad digital, el clásico engaño a una persona y el error que la induce a entregar su patrimonio desaparecen. Aquí, el engaño humano es sustituido normativamente por la "manipulación informática o artificio semejante", donde el sujeto activo altera directamente un sistema o algoritmo para que este realice la transferencia no consentida. Se trata de un delito puramente doloso y guiado por un evidente ánimo de lucro, donde el principal reto de imputación objetiva es demostrar con precisión técnica que la manipulación tecnológica creó un riesgo desaprobado por el derecho que provocó directamente el perjuicio financiero, el cual suele ejecutarse mediante redes criminales transnacionales y tácticas de *phishing*.

Finalmente, el trabajo demuestra que de nada sirve tener una teoría penal sólida si no sabemos procesar el delito. Debido a que la conducta delictiva se desmaterializa en la red, la evidencia digital se convierte en el verdadero motor del proceso penal. Tomando como base el artículo 259-A del Código Procesal Penal, analizo las complejidades de trabajar con elementos tan volátiles e intangibles como los registros de navegación, correos electrónicos y direcciones IP. La conclusión en este punto es contundente: el éxito del caso depende enteramente del respeto riguroso a la

cadena de custodia (artículo 250 Pr.Pn.) y de la idoneidad de la pericia informática para evitar que la prueba sea desvirtuada o declarada inadmisible. Asimismo, el estudio valida la necesidad de que la política criminal salvadoreña evolucione hacia técnicas especiales de investigación, como el Agente Encubierto Digital, siempre y cuando se ejecuten bajo un estricto control judicial que respete los límites constitucionales de la intimidad y el secreto de las comunicaciones, garantizando así un equilibrio real entre la eficacia penal y las garantías del debido proceso.

I. CAPÍTULO I

ASPECTOS TECNICOS DE LAS TECNOLOGIAS DE LA INFORMACION Y SURGIMIENTO DE LOS DELITOS INFORMATICOS

Sumario: 1.1. Relación de las TICS, Informática e internet, 1.2. Aspectos técnicos de las tecnologías de la información 1.3. Cómo funciona la internet 1.4 Proceso de la información cuando se navega por la internet, 1.5 Surgimiento de los Delitos Informáticos.

En la era del internet de las cosas, la seguridad digital deja de ser materia solo de expertos y se vuelve una práctica cotidiana imprescindible para proteger nuestra información tanto dentro como fuera de internet, para no ser víctimas de delitos informáticos.

En este capítulo desarrollaremos conceptos claves que son necesarios para comprender la tipología de los delitos informáticos en su aspecto técnico y especialmente el delito de estafa informática, desarrollaremos aspectos vinculados a la informática, las tecnologías de la información y comunicación y el funcionamiento de la red de redes "la internet", esto con el objeto de comprender la infraestructura tecnológica a la que nos enfrentamos a la hora de investigar el delito de estafa informática.

1.1 Relación entre TICS, Informática e internet:

En nuestra era hiperconectada, conocer sobre seguridad digital no es algo exclusivo de personas expertas en tecnología, sino una práctica cotidiana necesaria que debemos implementar para protegernos dentro y fuera del internet, como ya hemos mencionado.

Además, en el ámbito jurídico es preciso conocer de este tema en particular dado que, es en esta infraestructura que se llevan a cabo las actividades ilícitas relacionadas con los delitos informáticos, y especialmente con el delito de estafa informática.

Las Tecnologías de la información y comunicación (TIC) según la Ley Especial contra Delitos Informáticos y Conexos hace referencia al *"conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros"*[1].

Si partimos de la definición anterior, las tecnologías de la información no solo se limitan al uso de computadoras y sistemas de comunicación, para almacenar y procesar datos, sino que, podemos aseverar que las TICS básicamente son la aplicación práctica de la informática, como herramienta que usamos para organizar, buscar, compartir y utilizar una determinada información (datos), incluyendo dentro de estas herramientas las aplicaciones de redes sociales, todo con el objetivo de solucionar alguna problemática o hacer más práctica diversas actividades cotidianas en los diferentes medios en que nos desenvolvemos.

Entonces si las TICS están vinculadas a la informática, tenemos aquí otro de los conceptos que debemos desarrollar y por ende debemos manejar en nuestra práctica diaria; la Real Academia Española la define como la "ciencia que estudia el tratamiento automático de

[1] Ley Especial contra delitos Informáticos y Conexos. (El Salvador: Centro de Documentación Judicial, 2016), articulo 3.

la información por medio de sistemas computacionales"[2] esto hace referencia al proceso complejo que atraviesan los datos, puesto que la información no es más que datos, en su forma más genérica, que va desde procesarlos, almacenarlos y compartirlos a través de cualquier dispositivo electrónico.

Para lograr ese objetivo de procesar esos datos, necesitamos de dos grandes componentes, que básicamente son los cimientos de la informática: el hardware y el software, es decir por un lado tenemos las herramientas materiales tangibles, los dispositivos electrónicos que utilizamos a diario, y por otro el diseño, desarrollo y aplicaciones de sistemas de cómputo, así como los procesos algorítmicos que permiten el lenguaje computacional.

La informática está hoy presente en casi todos los campos de la vida moderna, con mayor o menor rapidez, todos los ámbitos del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas informáticos, para ejecutar tareas que en otros tiempos se realizaban manualmente.

Unido a lo anterior y para el funcionamiento de las TICS y la informática entra en juego otro concepto de vital importancia **"la internet"** como red de redes, es la que hace posible el surgimiento de las TICS y la razón de ser de la informática.

Es importante tener un acercamiento a estos conceptos porque como manifestamos supra es este ámbito en el que se ejecuta la acción típica del delito de estafa informática, por tanto, es de vital importancia que se conozcan los alcances de las tecnologías de la información,

[2] Real Academia Española. Diccionario de la lengua española. 2024, acceso: 3 de mayo de 2025, https://dle.rae.es/inform%C3%A1tico

la informática y la internet y su aplicación práctica en las actividades que realizamos con normalidad, así como tener un dominio o conocimiento básico de estos temas.

Resumiendo, tenemos:

La informática es la base teórica de la TICS: Proporciona los conocimientos fundamentales sobre hardware, software, algoritmos y estructuras de datos que son necesarios para desarrollar y utilizar sistemas informáticos, además de las herramientas tangibles e intangibles para el funcionamiento de las TICS.

Las TICS aplican los conocimientos de la informática: Utilizan estos conocimientos para crear soluciones tecnológicas que resuelvan problemas del mundo real, son la aplicación práctica de la informática e Internet.

La internet como infraestructura principal de las TICS: internet es el canal por excelencia para la transmisión y el acceso a la información y comunicación que las TICS potencian y que se logra claro está a través de las herramientas de informática.

Es, en este contexto tecnológico, que dio origen con las primeras computadoras y su veloz evolución, el creciente aumento de la capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, el desarrollo de la internet, así como la investigación en el campo de la inteligencia artificial, es que se va a enmarcar el cometimiento del delito de estafa informática, como se desarrollara más adelante.

1.2 Aspectos técnicos de las tecnologías de la información, informática e internet.

Cada vez se asienta más la idea de que la tecnología de la información y la comunicación globalizada pueden ser utilizadas para cometer actos delictivos con un alcance transnacional. Es claro, que, así como aprovechamos los avances tecnológicos en diversos campos, las estructuras criminales también han evolucionado y reforzado su actuar con las herramientas y recursos que facilitan las TICS, al grado que la esfera de actuación de los criminales ha migrado al internet, donde buscan el anonimato en la interacción con sujetos, que tienen como objetivo el cometimiento de delitos.

Conocer de este tema en particular, se vuelve trascendental en el ámbito jurídico, dado que, es en esta infraestructura tecnológica, en la que converge estos tres grandes conceptos "TICS, Informática e internet", en la que se llevan a cabo las actividades ilícitas relacionadas con los delitos informáticos, y especialmente con el delito de estafa informática.

¿Que nos interesa de estas correlaciones *"TICS, Informática e internet"* para este estudio practico?, bueno nos interesa recalcar los conceptos claves que se desprenden de cada uno así:

- ✓ **Sistema informático:** Es el conjunto de elementos necesarios para la realización y utilización de aplicaciones informáticas. Está integrado por cuatro elementos principales: ***Equipos (hardware) Programas (software) Firmware y Personal* informático**.[3]

[3] Francisco Jose Villazan Olivares. *Manual de Informática I (*Mexico: Hidalgo, Universidad Michoacana de San Nicolas Hidalgo, 2009),10.

Está constituido por aquellos componentes que permiten el funcionamiento de la informática como tal y por ende las TICS.

- ✓ **Hardware:** Es el conjunto de piezas físicas que integran una computadora: unidad central de proceso, placa base, periféricos y redes[4]. Se trata pues de los componentes físicos de un sistema informático, como computadoras, dispositivos de almacenamiento, incluyendo también a los teléfonos celulares, Tablet, y cualquier otro dispositivo móvil, con el que llevemos a cabo cualquier función con las TICS.

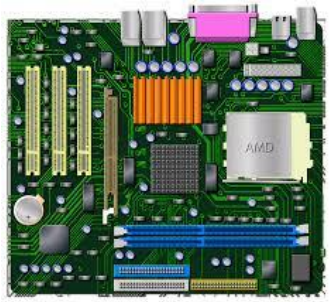
[4] Ibid

- ✓ **Unidad de proceso central (C.P.U.)**. Se le conoce como procesador o CPU su función es controlar, coordinar y llevar a cabo todas las operaciones del sistema[5].

  En palabras sencillas podemos decir que es como un chip que se encuentra en los dispositivos electrónicos.

- ✓ **Placa base.** Llamada tarjeta madre, es la tarjeta principal que contiene los componentes esenciales de un sistema de computación. Es el conjunto de circuitos impresos, chips y conectores. Aquí se localizan el procesador y la memoria principal, entre otros elementos.[6]

Es como el sistema nervioso de tu computadora, es lo que conecta el procesador (CPU) con la memoria AM y los órganos de almacenamiento (discos duros).



[5] Ibid. 11
[6] Ibid

- ✓ **Periféricos.** Son dispositivos que transmiten datos entre diferentes medios de información. Mediante los periféricos, la CPU guarda información y se puede comunicar con el mundo exterior[7].

  Son todos los accesorios de una computadora o dispositivo electrónico a través de estos se recibe, extrae, guarda, comparte o envía información.

Redes: Las infraestructuras que permiten la comunicación entre dispositivos.[8]

Una red es un conjunto de dispositivos (a menudo denominados nodos) conectados por enlaces de un medio físico, ya sea guiado (cables), o no guiados (de conexión inalámbrica).

[7] Ibid.12
[8] Andrew S. Tanenbaum y David J. Wetherall, *Redes de computadora* (Mexico, Pearson quinta edición, 2012), 2.

Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red.

Las redes según su tecnología pueden ser:

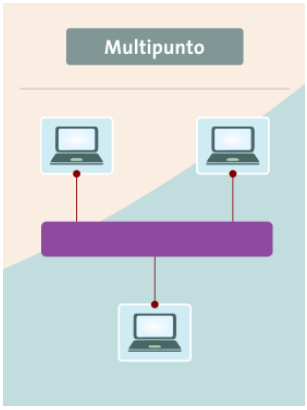
Punto a punto

Según Behrouz Forouzan es aquella "que proporciona un enlace dedicado entre dos dispositivos. Toda la capacidad del canal está reservada para la transmisión entre dos dispositivos"[9]. Estas redes, por lo general, están conectadas por cable, pero también es posible la conexión vía microondas.

Multipunto

También denominada multiconexión, "es una configuración en la que varios dispositivos comparten el mismo enlace y la capacidad de transmisión del canal en el espacio o el tiempo" [10]**.** Si los dispositivos pueden usar el enlace de forma simultánea se dice que hay una configuración de línea compartida espacialmente, pero si tienen que compartir la línea por turnos se trata de una configuración de tiempo compartido.

[9] Forouzan, Behrouz A y Sophia Chung Fegan. *Data Communications and Networking,* (EE.UU, Mc Graw-Hill Education, 2013),547.
[10]Ibid.



Redes según su alcance-extensión territorial que abarcan

Redes de área local (LAN)

LAN son las siglas de Local Área Network, red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios)[11].

Es una red de comunicación pequeña y privada para todos tus dispositivos electrónicos, podría ser tu casa, oficina, un salón de clases, o un espacio pequeño y limitados en el que convergen varios dispositivos que necesitan comunicarse entre sí.

Redes de área metropolitana (MAN)

Las redes de área metropolitana comprenden una ubicación geográfica determinada "ciudad o municipio" y su distancia de cobertura es mayor de 4 Km. Son redes con dos buses

[11] Universidad de Sevilla: 2. Redes de comunicación.pdf, acceso 27 de junio de 2025, https://biblus.us.es/bibing/proyectos/abreproy/70427/fichero/2.+Redes+de+comunica.ci%C3%B3n.pdf

unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos[12].

Un ejemplo de redes tipo MAN son las redes CATV o redes de televisión por cable. Al principio eran sistemas de carácter local con fines específicos, posteriormente, tras el impulso que supusieron para el desarrollo de importantes negocios de difusión, se inicia el cableado de ciudades enteras bajo concesión de los gobiernos[13]. Con la llegada del internet, los operadores de las redes se dieron cuenta de que, con algunos cambios en el sistema, podrían también proporcionar este servicio, aspecto que fue señalada por Andrew Tanenbaum.

Redes de área extensa (WAN)

Una red de área amplia puede ser descrita como un grupo de redes individuales conectadas a través de extensas distancias geográficas[14]. Los componentes de una red WAN típica incluyen:

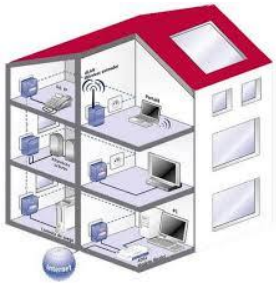
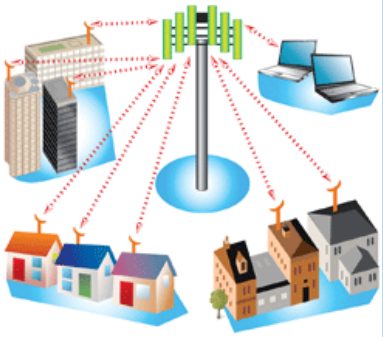
- Dos o más redes de área local (LANs) independientes.
- Routers conectados a cada LAN.
- Dispositivos de acceso al enlace (Link access devices, LADs) conectados a cada router.
- Enlaces inter-red de área amplia conectados a cada LAD.

[12] Ibid

[13] Andrew S. Tanenbaum y David J. Wetherall, *Redes de computadora* (México, Pearson quinta edición, 2012), 4.

[14] Universidad de Sevilla: 2. Redes de comunicación.pdf, acceso 27 de junio de 2025, https://biblus.us.es/bibing/proyectos/abreproy/70427/fichero/2.+Redes+de+comunica.ci%C3%B3n.pdf

Básicamente es una red de comunicación que abarca grandes distancias geográficas, es como una versión mucho más grande y extendida de una red LAN, y claro al abarcar una gran distancia es necesario otro tipo de tecnología que las conecte entre sí, entra aquí la fibra óptica. satélites, tecnologías celulares como 4g o 5g., dado que estas redes conectan al mundo entero.

		
LAN	**MAN**	**WAN**

✓ **Software:** Contiene las instrucciones que le permiten al equipo físico realizar una tarea específica. Están entregados por varios archivos que realizan diversas funciones. Hay tres tipos de software: los sistemas operativos, los lenguajes de programación y las aplicaciones informáticas.[15]

Es decir que es la parte no física de una computadora o dispositivo electrónico, si queremos hacer el símil se diría que el software es como el cerebro o la mente de los aparatos que les permite que sean funcionales.

[15] Ibid.11

Los softwares se clasifican según su función en:

Software de sistema. Programas que dan al usuario la capacidad de relacionarse con el sistema, para ejercer control sobre el hardware. El software de sistema también se ofrece como soporte para otros programas. Por ejemplo: sistemas operativos o servidores.

Software de programación. Programas diseñados como herramientas que le permiten a un programador desarrollar programas informáticos. Se valen de técnicas y un lenguaje de programación específico. Por ejemplo: compiladores o editores multimedia.

Software de aplicación. Programas diseñados para realizar una o más tareas específicas a la vez, pueden ser automáticos o asistidos. Por ejemplo: videojuegos o reproductores multimedia.

Forman parte del software de aplicación todos aquellos programas que no tienen que ver con el funcionamiento de la computadora, sino que se incorporan al sistema para que funcione como herramienta de trabajo (hoja de cálculo, procesador de palabras, programas de diseño gráfico, etc.), de ocio (videojuegos, reproductores de audio o video, etc.) o de información (enciclopedias digitales, navegador de internet, etc.), entre otras muchas funciones posibles

1.3 Como funciona la internet

Internet es una red de redes. Es un conjunto de redes de comunicación interconectadas entre sí, que enlazan ordenadores de todo el mundo, lo que permite compartir datos y recursos. En áreas reducidas los ordenadores suelen estar unidos entre sí por cables, pero cuando la zona a cubrir es más extensa, las conexiones se realizan a través de líneas telefónicas o satélites según Conceptos Básicos sobre Internet[16].

Con Internet podemos enviar mensajes, programas ejecutables, ficheros de texto, consultar catálogos de bibliotecas, pedir libros, hacer compras, enviar correos, etc; todos los recursos que se pueden encontrar en Internet existen porque alguna persona de forma voluntaria ha dedicado su tiempo en generarlos.

[16] "Conceptos Básicos sobre Internet", acceso el 25 de junio de 2025. https://www3.uji.es/~pacheco/INTERN~1.html.

Internet tuvo su origen en la década de los sesenta en la red experimental de la Agencia de Proyectos de Investigación ARPANET, del Departamento de Defensa norteamericano. Su objetivo era diseñar protocolos de comunicaciones que resolvieran los problemas locales que tenía dicho departamento.

ARPANET se popularizó y extendió entre algunos centros científicos y agencias del gobierno americano. Muchos organismos estatales y privados comenzaron a construir sus redes corporativas utilizando el mismo protocolo de conexión que esta red.

En poco tiempo, ARPANET empezó a utilizarse al margen de la finalidad inicial y los usuarios fueron creando nuevas herramientas. El tráfico de información que se generó fue creciendo con tal rapidez que obligó a mejorar las líneas de conexión.

Internet está en continuo proceso de cambio, cada día aparecen nuevas herramientas y se amplía la velocidad de sus conexiones.

1.4 Proceso de la información cuando se navega por la internet

1. Todo inicia cuando desde tu dispositivo electrónico (computadora, celular o tablet) abres tu navegador y entras a una página electrónica, usas un buscador o accedes a tus redes sociales.

Un navegador web o explorador web es "*una aplicación de software que permite al usuario acceder, visualizar, interactuar y navegar por páginas web en Internet. Su función*

principal es interpretar el código HTML, CSS, JavaScript y otros lenguajes web para presentar los contenidos de forma comprensible y accesible"[17].

A su vez una página web o página electrónica o página digital "es un documento de carácter multimediático**,** es decir, capaz de incluir audio, video, texto y sus combinaciones, que presenta su información de manera organizada y se encuentra alojado en internet**".** Se trata del formato básico de contenidos en la *World Wide Web* (WWW).[18]

Por ejemplo, quiero ver las noticias que salen en el periódico de mi elección, entonces ingreso a través de mi computadora, con el navegador Chrome y digito la página web de la prensa gráfica por ejemplo www.prensagrafica.com

[17]"Euskadi.Eus: Navegadores Web, servicios web, acceso 20 de mayo de 2025," https://www.euskadi.eus/navegadores-web/web01-a2wz/es/.

[18] Ibid..

Bastara un clic para que me aparezca el sitio de mi elección donde encontrare la información que estoy buscando.

2. Tu dispositivo envía al modem tu solicitud y, a su vez, el modem envía a tu compañía proveedora de internet (conocida también como ISP) la solicitud.

Un proveedor de servicios de Internet (ISP) es una empresa u organización que les proporciona a las personas, las empresas u otras organizaciones el acceso a Internet, por medio de una variedad de tecnologías como banda ancha, DSL, cable, fibra óptica, satélite y conexiones inalámbricas[19].

Los ISP brindan una variedad de servicios, como:

- Correo electrónico

- Alojamiento web

- Registro de nombres de dominio

- Redes privadas virtuales (VPN)

- Antivirus y software de seguridad

Proveedor
AMNET DATOS
TELEFONICA
SALTEL
TELECAM
INTERCOM
TELECOM
TELEMOVIL
INTELFON
DIGICEL
NAVEGA
SALNET
AMERICATEL
GCA TELECOM, S.A
GBM EL SALVADOR

[19]"Concepto: ISP concepto, tecnologías ISP, acceso el 15 de mayo de mayo de 2025": https://concepto.de/isp/

- Copias de seguridad en línea

- Almacenamiento en la nube

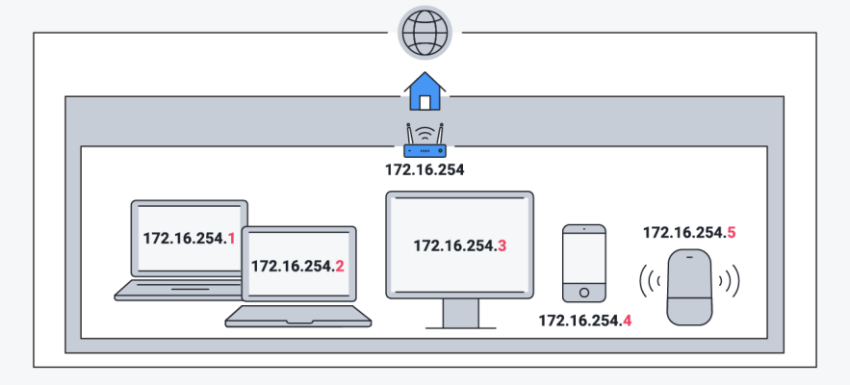
Cada vez que haces una solicitud/búsqueda, tu computadora o celular envían diversa información para identificarte. Esta información incluye qué página de internet quieres visitar, el modelo de tu dispositivo, de dónde estás haciendo la búsqueda y, dependiendo de las páginas que estás visitando, también cierta información personal.

¿Como se logra esto? A través de la IP, que Behrouz Forouzan lo define como un número único que identifica a un dispositivo (como una computadora, smartphone o servidor) dentro de una red que utiliza el protocolo de Internet para la comunicación. Sirve para localizar y diferenciar dispositivos en una red[20].

Las direcciones IP identifican y diferencian los miles de millones de dispositivos en línea, incluidos los ordenadores y los teléfonos móviles, y ayudan a esos dispositivos a comunicarse entre sí.

Con las direcciones IP se garantiza que los datos transmitidos se dirigen hacia la ubicación adecuada. De la misma manera que es necesaria una dirección postal para recibir y enviar cartas por correo, los dispositivos conectados a Internet requieren una dirección digital para recibir y enviar datos.

[20] Forouzan, Behrouz, "Comunicación de datos y redes de computadoras"*, Revista* McGraw-Hill Education, (2017). 5



Las direcciones IP suelen consistir en cuatro números del 0 al 255, separados por puntos. Dentro de cada dirección IP, puede ver el **ID de red**, asignado a su red por su ISP, y el **ID de host**, el identificador único asignado a cada dispositivo conectado a esa red específica.

172.16.254.1

El **ID de red** es la parte de una dirección IP con la que se identifica la red que se está utilizando para conectarse a Internet (**172.16.254.1**en el ejemplo anterior). El ID de red lo asigna un proveedor de servicios de Internet (ISP, por sus siglas en inglés) en el caso de conexiones domésticas a través de un router inalámbrico, por una red de empresa cuando la conexión se efectúa en el lugar de trabajo o por una red pública si la conexión se lleva a cabo en una cafetería Starbucks, por ejemplo.

Una red puede ser tan pequeña como dos ordenadores conectados entre sí o tan grande como Internet en sí, esto ya lo analizamos supra.

La parte del **ID de host** de una dirección IP indica el dispositivo concreto que está usando para conectarse a su red (es el «1» al final en el ejemplo anterior).

Por ejemplo, en casa tiene una serie de dispositivos y todos ellos requieren una dirección IP para conectarse a Internet. La configuración de estas direcciones IP podría parecerse al caso siguiente:

Nombre del dispositivo: **ID de red.ID de host**

Portátil1**: 172.16.254.1**

Portátil 2: **172.16.254.2**

Sobremesa: **172.16.254.3**

Smartphone: **172.16.254.4**

Altavoz inteligente: **172.16.254.5**

Para cada host (dispositivo) de una red, la parte de red de la dirección IP es la misma, mientras que el último número es distinto para identificar cada host. Un host tiene únicamente una dirección IP; una red tiene muchas.

3. Tu solicitud e información viajan de tu ISP a computadoras especializadas llamadas servidores, donde están almacenados los datos de la página que quieres visitar. Estos servidores almacenan una gran cantidad de información y se encargan de encontrar la información que estás buscando.

4. Una vez que encuentran la información, los servidores envían a tu ISP la información, la cual a su vez pasa a tu módem y finalmente a tu dispositivo electrónico.

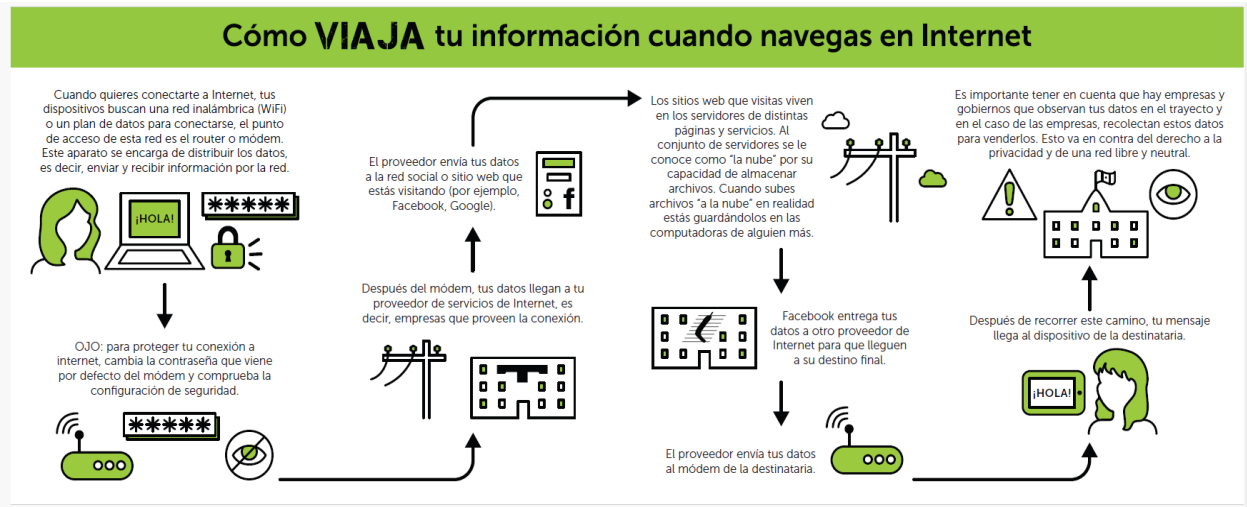
5. Toda esta información viaja por medio de algo conocido como "código html", que es el lenguaje que utilizan las computadoras para pasar de código binario (0's y 1's) a imágenes, texto, videos, etc.

Para comprender esto en términos sencillos, hagamos el esfuerzo de pensar en las computadoras como si hablaran un idioma secreto, este sería el código binario (0s y 1s) que no es más que el idioma más básico de las computadoras. Es como si solo pudieran usar dos palabras: "sí" (1) y "no" (0); entonces toda la información, ya sean letras, imágenes o videos, se traduce a esta serie de 0s y 1s

Por otro lado, el código HTML vendría a ser como un traductor cuya función es tomar ese complicado idioma de 0s y 1s y lo convierte en algo que nosotros, los humanos, podamos entender.

Es como un conjunto de instrucciones que le dicen al navegador web (como Chrome o Firefox o el que uses) cómo mostrar la información en la pantalla.

Por ejemplo, el HTML le dice al navegador: "Aquí va un párrafo de texto", "Aquí va una imagen", o "Aquí va un video" que además se adecua al tipo de dispositivo del que te estas conectando para que acorde a esas características se te pueda presentar.



1.5 Surgimiento de los Delitos informáticos

La revolución tecnológica trajo consigo cambios en todos los aspectos de la vida cotidiana y si vamos más allá, el mundo del deber ser tampoco se quedó atrás, la tecnología en los términos más generales y sus implicaciones en la vida cotidiana han obligado al legislador prácticamente, a establecer conductas penalmente relevantes, creando tipos penales que hace diez años eran impensables. Es claro que la criminalidad se ha innovado y ha adoptado nuevos patrones de comportamiento, ha reformulado su estructura organizacional, el reclutamiento, la financiación, la comunicación, conductas delictivas, y por medio de las nuevas tecnologías ha mejorado sus estrategias operacionales, mediante el uso de la encriptación, las criptomonedas y darkweb, dando lugar en el mundo del derecho al surgimiento de los delitos informáticos.

Ahora en el ámbito internacional a través de múltiples organismos multilaterales se ha buscado definir y delimitar los citados delitos, la primera legislación que se conoce del tema fue realizada por la OCDE (Organización de Cooperación y Desarrollo Económico) en el año de 1983, titulado Delitos de Informática: análisis de la normativa jurídica"[21].

Dicho escrito reseña la legislación existente en ese momento y realizaba algunas recomendaciones para que los Estados miembros las siguieran, las cuales se plasmaron en una lista que contenía ejemplos del uso indebido de la tecnología; dentro de estas se puede mencionar la falsificación y el fraude electrónico, la reproducción de programas electrónicos,

[21] Jessica López, y Mónica Sáenz Figueroa,"La obtención de la prueba penal internacional en materia de delitos cibernético,(monografia de grado, Universidad Politecnico gran Colombiano. Colombia, 2018) 16. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://alejandria.poligran.edu.co/bitstream/handle/10823/1501/Ciberdelitos%2520%2528Monica%2520Saenz%2520-%2520Jessica%2520Lopez%2529-Ultima%2520version%2520corregida.pdf%3Fsequence%3D1%26isAllowed%3Dy&ved=2ahUKEwiE0Kjp2qmOAxXKRjABHSq6H9AQFnoECBgQAQ&usg=AOvVaw13trEuvZMGO2kee4ey-6nw

espionaje informático, utilización no autorizada de computadores entre otros, los cuales deberían estar prohibidos y sancionados en la legislación penal interna de cada país.

En el año de 1996 el Comité Europeo para los Problemas Criminales (CDPC), creó una comisión de expertos en materia de delitos cibernéticos. Su decisión se cimentó en aspectos tales como el vertiginoso desarrollo en el sector de la tecnología de la información, la compenetración de los sistemas de telecomunicación, y por último la facilidad en el acopio y transmisión de comunicación a través de redes y superautopistas de la información.

En este contexto, se empezó a dilucidar el concepto de delitos cometidos en el ciberespacio, los cuales contienen actividades que transgreden la confiabilidad, disponibilidad e integridad tanto de las redes, datos y sistemas informáticos entre otros bienes jurídicos vinculados a las TICS , esto llevó a que en el año 2001 se suscribiera en la ciudad de Budapest"[22]., el Convenio sobre la Ciberdelincuencia del Consejo de Europa en el cual se definen una serie de conductas delictivas encaminadas a abusar o violar la disponibilidad, confidencialidad e integridad, de los datos, redes y sistemas informáticos.

A partir del convenio de Budapest surgen dos corrientes vinculadas al tratamiento de este tipo de delitos, una corriente que pretende tratar al delito informático como una nueva rama del derecho penal, **modelo fenomenológico.** Y por otro lado existe la corriente que intenta integrar el tema de los delitos informáticos en el campo ya regulado por el derecho penal, introduciendo sólo modificaciones o ampliaciones legislativas necesarias en los tipos penales tradicionales, de manera tal de poder comprender en ellos la ejecución de los tipos por

[22] Convenio sobre la Ciberdelincuencia (Convenio de Budapest), (Consejo de Europa, 2001).

medio de mecanismos informáticos[23].**Vale decir que la primera corriente se centra en el fenómeno de la criminalidad y la segunda en el bien jurídico protegido**.

En nuestro país es claro que el legislador se ha inclinado por la primera de estas posturas, de ahí que ha querido contemplar los delitos informáticos en una legislación especial, abordando la criminalidad informática desde una rama especializada del derecho, es así que en el año 2016 se crea la Ley Especial contra delitos informáticos y conexos[24].

La creación de esta normativa fue motivada en parte porque el país comenzó a experimentar un aumento en la comisión de delitos a través de medios informáticos es decir a través del uso de las tecnologías de la información y comunicación, situaciones que la normativa penal existente hasta la fecha resultaba insuficiente para abordar la complejidad y las particularidades de estos nuevos tipos penales; no existía una ley que abordara de manera integral la ciberdelincuencia tal cual lo establecía el convenio de Budapest.

La Ley Especial contra delitos Informáticos y Conexos fue emitida mediante el decreto legislativo número 260 de fecha cuatro de febrero de 2016 y fue publicada en el Diario Oficial número 40 tomó 410 del 26 de febrero de ese mismo año.

Por tanto, esa normativa surgió como una respuesta legislativa crucial a la evolución y sofisticación de los crímenes cibernéticos buscando llenar un vacío legal de las normativas penales a la fecha, brindando herramientas más efectivas y novedosas para la persecución y la

[23] Ariel Devia, González Edmundo, Estafa informática del artículo 248.2 del Código Penal, (Tesis, Universidad de Sevilla, 2017) 468.

[24] Ley Especial contra delitos Informáticos y Conexos. (El Salvador: Centro de Documentación Judicial, 2016) articulo 1.

sanción de estas conductas que están directamente vinculadas al ámbito digital y nuevas tecnologías.

Partiendo de esta especialidad lo fundamental es comenzar por establecer un concepto claro de delito informático como tal, y para lograr este cometido, comenzaremos por definir tres conceptos que son clave para poder construir una definición de delito informático, estos son: información, informática y datos.

La Real Academia Española define estos conceptos de la siguiente manera:

Información como "la comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada"[25].

Del mismo modo, define *informática* como "el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores." Y por otro lado, indica que dato "es la Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho"; información dispuesta de manera adecuada para su tratamiento por un ordenador[26].

Partiendo de lo anterior podríamos definir el delito informático, **como aquel que tipifica cualquier acto del ser humano como ilícito, cuando el mismo tiene por fin perturbar o afectar datos, información o sistemas de información teniendo como consecuencia el daño directo o indirecto en ellos, así como también el mal uso de los mismos.**

[25] "Real Academia Española. Diccionario de la lengua española. 2024". Acceso el 20 de mayo de 2025, https://dle.rae.es/inform%C3%A1tico.
[26] Ibid

Siguiendo a ROMEO CASANOVA, quien refiere que con la expresión delitos informáticos, suele aludirse a "conductas que atentan de forma grave a determinados bienes del individuo, pero también de persona jurídica que presentan una configuración específica y exclusiva de la actividad informática y telemática, una tipología técnico-criminológica, que se caracteriza por acceso, alteración, ocultación o destrucción no autorizados de los datos almacenados en un sistema informático; reproducción completo parcial de datos contenidos en un sistema informático; creación de un fichero clandestino; venta de ficheros informáticos; sustracción del tiempo de sistemas informáticos o telemáticos, etcétera"[27].

Por su parte la ley Especial de Delitos informáticos y conexos, en su artículo 3 define así: "*a) Delito Informático: se considerará la comisión de este delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información*;"[28].

La ley define los delitos informáticos como aquellas conductas ilícitas que se realizan mediante el uso de tecnologías de la información y comunicación, afectando bienes jurídicos como la información, los sistemas informáticos, la propiedad, la privacidad, entre otros; se enfoca en proteger los bienes jurídicos que pueden ser vulnerados por el uso de tecnologías de la información.

[27] Carlos Romeo, Casanova. *Enciclopedia Penal Básica.*(Granada: Comares, 2002), 518.

[28] *Ley Especial contra delitos Informáticos y Conexos.* San Salvador, San Salvador: Centro de Documentación Judicial, 2016.

Se tipifican conductas delictivas que se realizan tanto a través de internet como de otros medios informáticos.

Partiendo de la Ley Especial contra Delitos Informáticos y Conexos, la cual sistematiza los tipos penales relacionados con la ciberdelincuencia, podemos clasificar los delitos informáticos de la siguiente manera:

A. los Delitos contra los Sistemas Tecnológicos de Información.

1) Acceso indebido a sistemas informáticos (Art. 4).

2) Acceso indebido a los programas o datos informáticos (Art. 5).

3) Interferencia del sistema informático (Art. 6).

4) Daños a sistemas informáticos (Art. 7).

5) Posesión de equipos o prestación de servicios para la vulneración de la seguridad (Art. 8)

6) Violación de la seguridad del sistema (Art. 9).

B. Los delitos informáticos

7) Estafa informática (Art. 10).

7) Fraude informático (Art. 11).

8) Espionaje informático (Art. 12).

9) Hurto por medios informáticos (Art. 13).

10) Técnicas de denegación de servicio (Art. 14).

C. Delitos informáticos relacionados con el contenido de los datos

11) Manipulación de registros (Art. 15).

12) Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (Art. 16).

13) Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medos similares (Art. 17).

14) Provisión indebida de bienes o servicios (Art. 18).

15) Alteración, daño a la integridad y disponibilidad de datos (Art. 19).

16) Interferencia de datos (Art. 20).

17) Interceptación de transmisiones entre sistemas de las tecnologías de la información y la comunicación (Art. 21).

18) Hurto de identidad (Art. 22).

19) Divulgación no autorizada (Art. 23).

20) Utilización de datos personales (Art. 24).

21) Obtención y transferencia de información de carácter confidencial (Art. 25).

22) Revelación indebida de datos o información de carácter personal (Art. 26).

23) Acoso través de tecnologías de la información y la comunicación (Art. 27).

D. Delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad.

24) Pornografía a través del uso de tecnologías de información y la comunicación (Art. 28).

25) Utilización de niñas, niños y adolescentes o personas con discapacidad en pornografía a través del uso de tecnologías de información y la comunicación (Art. 29).

26) Adquisición o posesión de pornografía de niñas, niños, adolescentes o personas con discapacidad a través del uso de tecnologías de información y la comunicación (Art. 30).

27) Corrupción de niñas, niños, adolescentes o personas con discapacidad a través del uso de tecnologías de información y la comunicación (Art. 31).

28) Acoso a niñas, niños y adolescentes o personas con discapacidad a través del uso de tecnologías de información y la comunicación (Art. 32).

29) Condiciones agravantes comunes (Art. 33).

E. Delito contra el orden económico

30) Suplantación en actos de comercialización (Art. 34)

La clasificación de los delitos informáticos en El Salvador, establecida en la Ley Especial contra los Delitos Informáticos y Conexos, atiende a varios propósitos fundamentales:

- **Protección de bienes jurídicos:**

La clasificación busca proteger diversos bienes jurídicos que pueden ser vulnerados a través del uso de tecnologías de la información. Esto incluye la confidencialidad, integridad y disponibilidad de los datos, la propiedad intelectual, la privacidad y la seguridad económica.

- **Tipificación de conductas delictivas:**

Permite identificar y definir de manera precisa las conductas que se consideran delitos informáticos. Esto facilita la labor de las autoridades encargadas de investigar y perseguir estos delitos.

- **Adecuación de penas:**

La clasificación establece una correspondencia entre la gravedad de los delitos y las penas aplicables. Esto garantiza que las sanciones sean proporcionales al daño causado.

- **Fortalecimiento de la seguridad cibernética:**

Al tipificar los delitos informáticos, se contribuye a crear un marco legal que disuade la comisión de estos delitos y promueve un entorno digital más seguro.

- **Adaptación a la evolución tecnológica:**

La clasificación busca adaptarse a la rápida evolución de las tecnologías de la información, permitiendo abordar nuevas formas de delitos informáticos que puedan surgir.

- **Protección de los niños y adolescentes:**

Uno de los puntos clave de la ley, es el de la protección a los menores en la red, protegiéndolos de delitos como la pornografía infantil, y otros delitos cometidos en la red.

En resumen, la tipificación de los delitos informáticos en El Salvador tiene como objetivo principal proteger a la sociedad de los riesgos que plantea el uso indebido de las tecnologías de la información, estableciendo un marco legal que permita prevenir, investigar y sancionar estos delitos.

2 CAPÍTULO II

GENERALIDADES DE LOS CRIPTOACTIVOS Y SU COMERCIALIZACIÓN

Sumario: 2.1 Surgimiento de las criptomonedas, 2.2 Cuestiones técnicas de los criptoactivos, 2.3 Como se entrelaza la criptografía y la blockchain, 2.4 ¿Cómo funciona una transacción con criptoactivos?, 2.5 Tipos de Billeteras de Criptomonedas**,** 2.6 Comercialización de criptoactivos, 2.7 Como podemos usar los criptoactivos, 2.8 Señales alertas relacionados a la comercialización de criptoactivos, 2.9 Debida diligencia en la comercialización de criptoactivos, 2.10 Entorno regulatorio de los criptoactivos en El Salvador

Este capítulo ofrecerá una visión general de los criptoactivos centrándose en sus aspectos fundamentales y cómo se compra vende y utilizan, se explicara el surgimiento de las criptomonedas seguido de cuestiones técnicas en las que se desarrollaran conceptos fundamentales para comprender la comercialización de los mismos y se profundizará en la relación crucial entre criptografía y blockchain y asimismo en el proceso de creación de billeteras, para finalmente abordar las consideraciones importantes relacionadas con el comercio de Criptoactivos incluyendo alertas relacionadas a su comercialización, el concepto de bebida diligencia en este contexto y el entorno regulatorio de los mismos.

2.1 Surgimiento de los Criptoactivos.

El origen de los Criptoactivos es un fascinante recorrido que entrelaza la criptografía, la informática y una visión revolucionaria del mundo financiero. No podemos hablar de Criptoactivos sin mencionar que este es el género y la especie son las “criptomonedas”, dado

que como veremos más adelante, los criptoactivos es un término amplio que abarca varios activos digitales, de los cuales las criptomonedas son la especie más usada en la práctica.

Hablar de criptomonedas es remontarnos a la década de 1980, en la que criptógrafos como David Chaum[29] comenzaron a explorar la posibilidad de crear dinero digital seguro y privado. Chaum, con su concepto de "eCash", sentó las bases para transacciones electrónicas anónimas, un principio fundamental de las criptomonedas.

En la década de 1990, figuras como Wei Dai[30] ingeniero informático conocido por sus contribuciones a la criptografía y las criptomonedas, desarrolló la biblioteca criptográfica Crypto, creó el sistema de criptomonedas b-money y co-propuso el algoritmo de autenticación de mensajes, y por otro lado Nick Szabo[31] continuo esta línea de pensamiento. Dai propuso "b-money", un sistema de efectivo electrónico descentralizado, mientras que Szabo concibió "bit gold", una moneda digital basada en la prueba de trabajo.

Aunque estos proyectos nunca se materializaron completamente, allanaron el camino para futuros desarrollos.

Es hasta el año 2008 que se acuña el concepto de criptomoneda como tal, con el nacimiento del Bitcoin, en medio de la crisis financiera que se origina en Estados Unidos pero que tuvo repercusiones en la economía mundial[32]; Una persona o grupo de personas bajo el

[29] "BASIC: ¿Quién es David Chaum? s.f." acceso 15 de mayo de 2025, https://academy.bit2me.com/quien-es-david-chaum/
[30] "Bitcoin it:Wei Dai, wiki de Bitcoin", acceso 20 de mayo de 2025, https://es.wikipedia.org/wiki/Wei_Dai;
[31] "Cointelegraph: quien es Nick Zsabo", acceso 20 de mayo de 2025, https://es.cointelegraph.com/news/nick-szabo-bitcoin-hbo-satoshi-nakamoto

seudónimo de Satoshi Nakamoto, publicó el "white paper"[33] de Bitcoin, este es un documento técnico que proporciona información detallada sobre la tecnología subyacente, objetivos, mecanismo de funcionamiento de la criptomoneda, viene a ser como una guía o la hoja de ruta de estos proyectos.

Este White paper describía un sistema de dinero electrónico peer-to-peer (p2p), descentralizado, anónimo, que eliminaba la necesidad de intermediarios financieros.

En 2009, se lanzó la red Bitcoin, lo que permitió que la primera criptomoneda comenzara a operar y por tanto fuera parte del ecosistema financiero; de ahí en adelante pues las criptomonedas se reprodujeron como espuma y comenzaron a ser parte de los medios de pago en la mayoría de las transacciones financieras, con esto también se creó el riesgo y el uso de las mismas en actividades delictivas.

El origen de las criptomonedas es una historia de visión, innovación y perseverancia. Desde los primeros criptógrafos que soñaron con un dinero digital seguro como medio de pago accesible a todas las personas, hasta la creación de Bitcoin y la explosión del ecosistema actual con la tecnología Blockchain, aplicada no solo a criptomonedas sino a otras facetas de las actividades humanas; las criptomonedas por tanto han transformado la forma en que pensamos sobre el dinero y las finanzas y sobre todo en como concebimos los actos de comercio.

2.2 Cuestiones técnicas de los criptoactivos.

[33] "Bitcoin.org: a peer to peer electronic cash system" , acceso 20 de mayo de 2025, https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf.

Para comprender como se comercializan los criptoactivos es imprescindible dominar e interrelacionar una serie de conceptos, que serán de utilidad para entender el universo cripto.

Comenzamos diciendo que los criptoactivos son el género "Son activos digitales que utilizan la criptografía para asegurar y verificar transacciones y para controlar la creación de nuevas unidades. Los criptoactivos se basan en la tecnología blockchain, que es un registro descentralizado y público de todas las transacciones realizadas con esa moneda digital. Los criptoactivos incluyen criptomonedas (como Bitcoin y Ethereum), tokens y otros activos basados en blockchain."[34].

Esto quiere decir que al hablar de criptoactivos no sólo se debe entender como criptomonedas dado que este es un concepto mucho más amplio, es un tipo de activo digital, es decir no son tangibles como el dinero fiduciario, basado como ya se dijo en la criptografía y además su valor no lo determina una entidad centralizada sino que el propio mercado.

Un activo digital o criptoactivos según Böhme, Christin, Edelman, & Moore "es un recurso en formato digital que tiene un valor y se puede almacenar, transferir o intercambiar de manera electrónica. Estos activos pueden incluir criptomonedas, tokens, archivos de medios digitales, documentos, imágenes, videos, bases de datos y cualquier otro tipo de contenido o archivo que tenga un valor económico o utilidad en plataformas digitales."[35].

[34] "Unir: ¿Qué son los criptoactivos?, acceso 20 de mayo de 2025, https://www.unir.net/revista/empresa/criptoactivos/
[35] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives. Páginas 213-238.

Dichos activos digitales pueden transferirse electrónicamente, utilizando un sistema de Tecnología de Registro Distribuida, o tecnología similar o análoga, en la cual los registros se encuentran enlazados y cifrados para proteger la seguridad y privacidad de las transacciones.

Desglosemos estas definiciones para una mejor comprensión de lo que es un criptoactivo, partimos que un activo digital es cualquier cosa que exista en formato digital y que tenga un valor, recordemos que nos encontramos en la era del internet del valor, todo lo que tenga una representación digital adquiere a la vez un valor, ubicamos a los criptoactivos como activos digitales, dentro de los cuales encontramos la especie "criptomonedas, tokens, NFT, por mencionar algunos y que desarrollaremos más adelante.

Que tienen en común los criptoactivos, que están basados en criptografía y tecnología Blockchain, extraigamos estos dos conceptos.

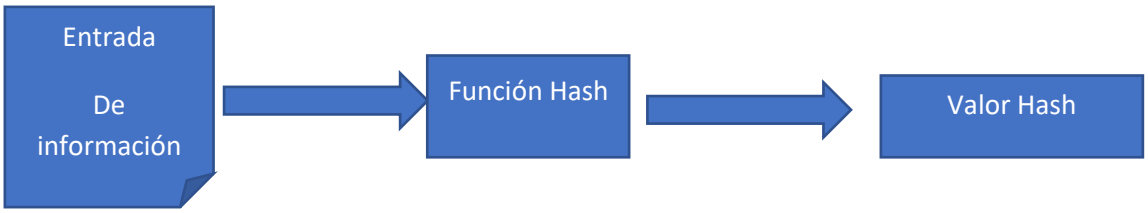
La criptografía es *"la ciencia de representar información de forma opaca para que solo los agentes autorizados (personas o dispositivos diversos) sean capaces de desvelar el mensaje oculto*[36]. El proceso de ocultar la información se llama cifrado o encriptado y el proceso de desvelarla se llama descifrado o desencriptado.

¿Como funciona esto en el mundo de las criptomonedas?

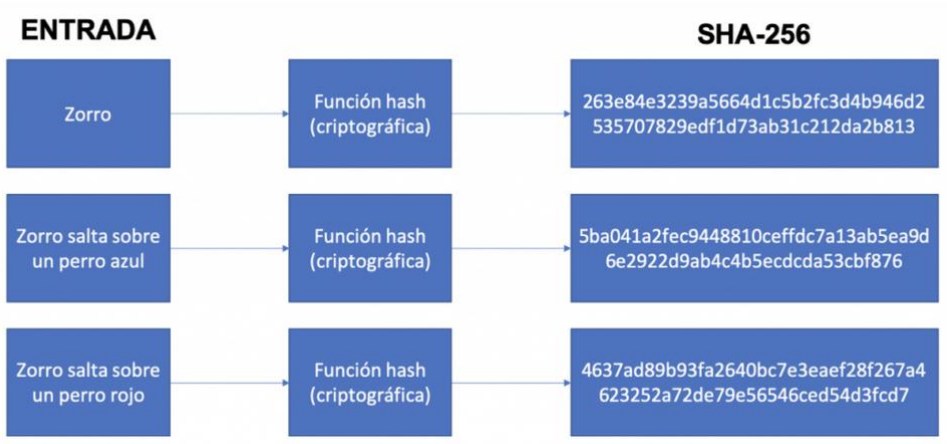
Este pilar fundamental del mundo cripto tiene su cimiento en las funciones hash, es decir, es necesario un mecanismo que permita encriptar información, y este es precisamente la

[36] "Bit2Me Academy: Obtenido de ¿Qué es una wallet o monedero de criptomonedas?", acceso 20 de mayo de 2025, https://academy.bit2me.com/wallet-monederos-criptomonedas/

función hash, que no es más que *"algoritmos que transforman cualquier cantidad de datos en una cadena de caracteres alfanuméricos de una longitud fija"*[37].



Es decir, que cualquier información o dato a través de la función hash se puede transformar en una codificación alfanumérica que la cifra, la cubre la encripta, y no importa la longitud de la información de entrada esta siempre dará una salida con una longitud fija.



Esta función hash es un algoritmo que permite esa conversión, y garantiza que estos códigos sean irrepetibles, es lo que permite por ejemplo que que tu contraseña en Facebook sea distinta y segura respecto a la de tu amigo o familiar, aunque todos usen la misma plataforma.

[37] Ibid

En la actualidad, se utilizan diversos tipos de algoritmos que se ajustan a diferentes tipos de necesidades. Entre los algoritmos hash más recomendables actualmente para proteger las contraseñas son los siguientes:

- Bcrypt
- sha512crypt
- sha256crypt[38]

Es decir que los anteriores son ejemplos de algoritmos que permiten cifrar de manera efectiva contraseñas. permitiendo construir una plataforma de seguridad de contraseñas que evoluciona junto con la tecnología de informática, para protegerse contra las amenazas futuras, como la posibilidad de que los atacantes tengan la capacidad de procesamiento para descifrar.

De manera que la criptografía no es más que el arte de ocultar o proteger información para que solo determinadas personas autorizadas puedan acceder a la misma, viene a ser como un lenguaje secreto que convierte información normal en algo incomprensible y solo con una clave especial se puede volver legible, esto garantiza, confidencialidad, integridad y autenticación en el mundo cripto.

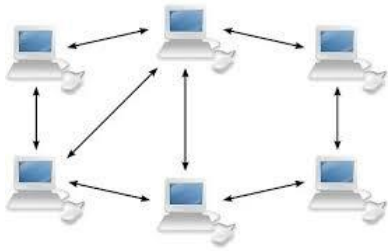
Luego de entender la criptografía corresponde desarrollar el otro concepto "la Blockchain", *que es un gigantesco libro de contabilidad distribuido (DLT) en el que los registros (bloques) están enlazados para proteger la seguridad y la privacidad de las*

[38] "SecuriHub: ¿Qué es un Hash? Criptografía para principiantes", https://securihub.com/que-es-un-hash-criptografia-para-principiantes/

transacciones. Se trata de una base de datos distribuida y segura gracias a la utilización de algoritmos criptográficos[39].

Esta base de datos distribuida está constituida por usuarios conectados con sus equipos (computadoras) que forman esta red interconectada; a estos usuarios se les denomina nodos.

Un nodo es la base fundamental de la tecnología blockchain. Por medio de estos podemos crear una enorme red de computadores interconectadas que comparten información de forma segura, rápida y descentralizada, y nos permiten disfrutar de todas las ventajas de la cadena de bloques.



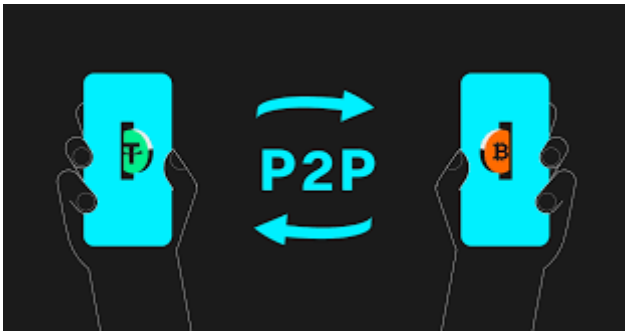
Así, desde el punto de vista de la tecnología blockchain (cadena de bloques) y las criptomonedas, los nodos son los ordenadores que están interconectados a la red de una criptomoneda, ejecutando el software que se encarga del funcionamiento.

Para lograr esta conexión, los nodos de blockchain se comunican entre sí por medio de protocolos P2P, lo que garantiza que cualquier persona con el software adecuado puede formar parte de la red, sin que nadie pueda censurar su participación y acceso a los recursos de dicha red[40].

[39] "UIF: Unidad de Investigación Financiera: Guía de investigación de criptoactivos", acceso 18 de mayo de 2025, https://www.uif.gob.sv/

[40] "Bit2me Academy: ¿Qué es una red P2P?", acceso 16 de mayo de 2025, : https://academy.bit2me.com/que-es-una-red-p2p/

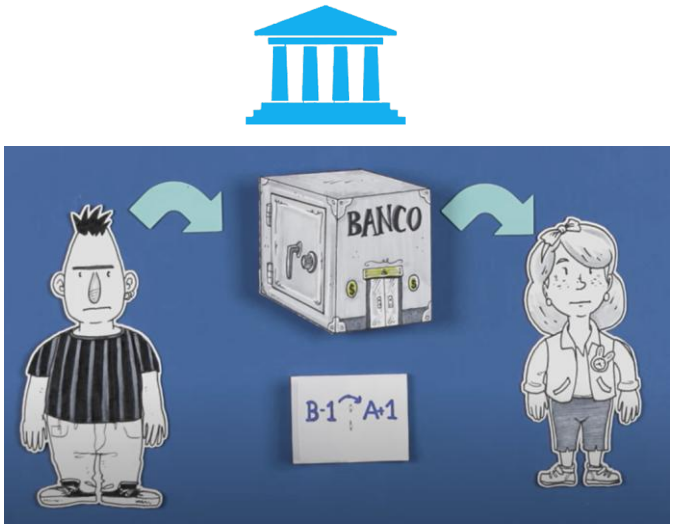
Cuando desarrollamos los conceptos básicos de informática, nos detuvimos en el lenguaje computacional o informático que es parte fundamental de la comunicación en la red o internet, pues un protocolo P2P es exactamente eso, es un modelo en el que cada uno actúa tanto como cliente o como servidor, interconectados entre sí.



Existen varios tipos de nodos, cada uno con diferentes roles dentro de la red blockchain; entre los cuales se encuentra los nodos mineros crean y proponen nuevos bloques dentro de la red blockchain, mientras que los nodos validadores buscan verificar y aprobar las nuevas transacciones que se van generando en este ecosistema.

2.3 Como se entrelaza la criptografía y la blockchain

Para comprender esta intercalación es preciso que expliquemos primero como funciona una transacción en dinero FIAT o dinero contante y sonante.



A quiere enviar dinero a **B** y esto lo realiza a través de una transacción en línea desde su cuenta bancaria hacia la cuenta bancaria de **B**. En este proceso ocurre lo siguiente:

1. Hay un ente central que es el banco que valida que **A** tenga primeramente una cuenta en el sistema financiero que le habilite a realizar la transacción, y en segundo lugar que tenga los fondos en su cuenta que desea transferir a **B.**

2. De igual manera el banco valida que **B** tenga una cuenta bancaria que permita recibir la transferencia que le hará **A**.

3. **"B"** le proporciona el número de cuenta a **"A"** para que pueda realizar la transferencia

4. Cuando los fondos se encuentran en la cuenta de **B** este puede accesar a los mismos a través de su **clave única** que les es proporcionada como titular de la cuenta para que acceda a los mismos a través de su banca en línea. **(esta clave o contraseña es única e intransferible).**

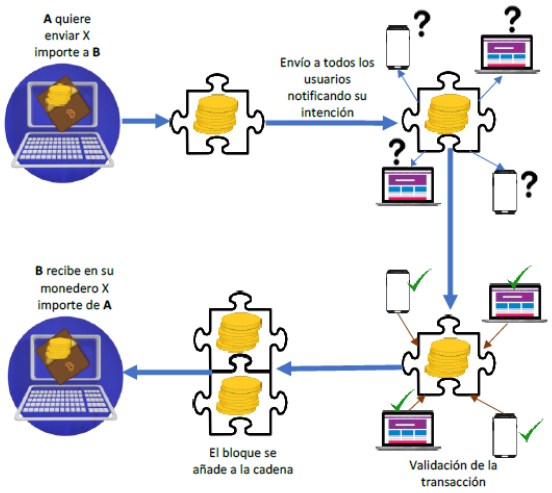
5. Esta transacción queda reflejada en el Estado de cuenta de **A y B** y puede solicitarse si se desea al banco que pertenece cada una de las cuentas.

6. Por último, en todo este proceso hay un sujeto que no vemos y que tiene una función de vigilante en cuanto al cumplimiento de toda la legislación pertinente a través de las diversas entidades que es el Estado mismo.

2.4 ¿Como funciona una transacción con criptoactivos?

Ahora veamos cómo funciona esta misma transacción en el mundo cripto, y así terminamos de acuñar los términos que nos hacen faltan para completar la rompecabeza de las criptomonedas.

Partimos de la idea que las criptomonedas se emiten al margen de los gobiernos y bancos centrales y, al menos en teoría, esta función se traslada a todo aquel que quiera participar. Esta generación de moneda se denomina "minado". Estos participantes (nodos mineros) son quienes aportan la seguridad a las transacciones utilizando, en la mayor parte de los casos, la tecnología de blockchain.



1. **Partiendo del ejemplo anterior para que el mismo A pueda realizar una transacción a B necesita primeramente que ambos tengan una cuenta en el mundo cripto, esta cuenta se denomina BILLETERA O WALLET.**

El término wallet hace referencia a una cartera, billetera o monedero virtual en el que se puede gestionar los activos criptográficos. Es un software o hardware diseñado

exclusivamente para almacenar y gestionar las **claves públicas y claves privadas** de las criptomonedas[41].

Esto quiere decir que una billetera te permite interactuar con redes blockchain para enviar, recibir y gestionar activos digitales como criptomoneda, tokens, etc.; también se utilizan para generar y almacenar tus claves privadas y frases de recuperación, que son básicamente las contraseñas que te dan acceso a tus criptomonedas.

Detengámonos en las claves públicas y claves privadas:

La clave publica: Es una direccion que se puede compartir con otros usuarios para recibir pagos o transferencias de criptomonedas.

1BoatSLRHtKNngkdXEeobR76b53LETtpyT

Es una cadena de caracteres nica y extensa que se genera mediante la aplicacion de un algoritmo criptografico la clave privada correspondiente[42].

Es similar a un número de cuenta bancaria. Podemos entregarla a cualquier persona para que nos envíe dinero, sin el riesgo de que pueda extraer nuestros fondos. A través de la clave pública se generan direcciones para recibir, consultar y ver el estado de nuestros fondos.

[41] "Bit2me Academy: ¿Qué es una red P2P?",acceso el 15 de mayo de 2025, https://academy.bit2me.com/que-es-una-red-p2p/

[42] "Tech target: ¿Qué es una clave privada?, acceso 15 de mayo de 2025, https://www-techtarget-com.translate.goog/searchsecurity/definition/private-key?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

La clave privada es una contraseña (es decir, una cadena de letras y números) que permite acceder a sus fondos en criptomonedas y administrarlos[43]; funciona como una especie de llave, un PIN o contraseña que no debemos revelar a nadie, ya que nos otorga el derecho de gastar las criptomonedas contenidas en una dirección.

A manera de ejemplo podemos decir que la clave publica es como dirección de correo electrónico que uno proporciona para que te remitan un correo, y la clave privada es la contraseña con la que entras al correo para ver el contenido de los correos, entonces la clave privada es la que te permite mover tus activos.

Al crear una billetera se requerirá además que se escriban una serie de palabras **(frase semilla)**

Una frase semilla es un conjunto de palabras que **se utiliza como una clave secreta para acceder a una billetera de criptomonedas[44]**

La frase semilla es una forma de autenticar la identidad del usuario y proteger su acceso a la billetera.

Las frases semilla son generalmente una secuencia de 12, 18 o 24 palabras que se generan de manera aleatoria y se presentan al usuario durante el proceso de configuración de la billetera.

[43] Ibid
[44] "Bit2me Academy: ¿Qué es una red P2P?", acceso 16 de mayo de 2025, https://academy.bit2me.com/que-es-una-red-p2p

Es importante que el usuario escriba la frase semilla en un lugar seguro y no la comparta con nadie, ya que cualquier persona que tenga acceso a la frase semilla puede acceder a la billetera y a las criptomonedas almacenadas en ella.

2.5 Tipos de Billeteras de Criptomonedas

Existen muchos tipos de billeteras de criptomonedas. Algunas están disponibles en varios dispositivos, mientras que otras están diseñadas específicamente para un solo tipo de dispositivo, veamos:

- **Billeteras con custodia y billeteras sin custodia**

La mayoría de las billeteras de criptomonedas son con o sin custodia, y se diferencian principalmente en la propiedad y el control de las claves privadas.

Las **billeteras con custodia** son administradas por terceros, como exchanges de criptomonedas, que almacenan y gestionan las claves privadas en tu nombre. Estas billeteras priorizan la

comodidad y te permiten recuperar fondos más fácilmente si olvidas tu contraseña o pierdes el acceso[45].

Sin embargo, las billeteras con custodia requieren que confíes en la seguridad y fiabilidad del custodio, ya que no tendrás el control total de tus activos.

- Las **billeteras sin custodia**, por otro lado, te otorgan control total sobre tus frases de recuperación y claves privadas, lo que garantiza la propiedad total de tus criptomonedas. Esta independencia mejora la seguridad y la privacidad, pero conlleva una mayor responsabilidad[46].

En estas billeteras tu eres el custodio de tus claves, si tus claves se pierden o están en peligro, es casi imposible recuperarlas.

- **Billeteras de hardware:** son dispositivos electrónicos que utilizan un generador de números aleatorios (RNG) para generar claves públicas y privadas. A continuación, las claves se almacenan en el propio dispositivo. El almacenamiento de hardware es un tipo de billetera fría, lo que significa que funciona sin conexión y no está conectada a Internet cuando almacena y firma transacciones de criptomonedas.[47]

Este aislamiento de las redes en línea mejora la seguridad de las claves privadas y las protege de posibles amenazas en línea, como la piratería o los ataques de malware. Al mantener las claves

[45] Binance: Binance Academy, Wallet, acceso 15 de mayo de 2025, https://academy.binance.com/es/articles/crypto-wallet-types-explained

[46] Binance: Binance Academy, Wallet, acceso 15 de mayo de 2025, https://academy.binance.com/es/articles/crypto-wallet-types-explained

[47] Ibid

privadas fuera de línea, las billeteras de hardware proporcionan una capa adicional de protección, lo que las convierte en la opción preferida para las personas que buscan una mayor seguridad para sus activos digitales.

Algunos ejemplos populares de billeteras de hardware son Ledger, Trezor, Tangem y SafePal.

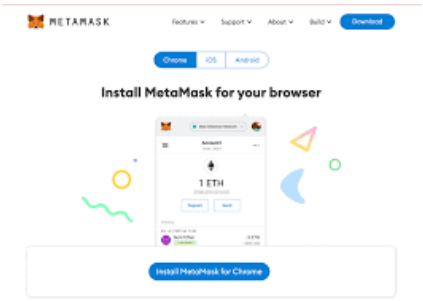
- **Billeteras de software**

Las billeteras de software vienen en una variedad de formas, incluyendo billeteras web, de escritorio y móviles. Ofrecen comodidad y accesibilidad, pero la mayoría son billeteras calientes, lo que significa que están conectadas a Internet de alguna manera.

Para mayor claridad, abordaremos los diferentes tipos de billeteras de software por separado, pero ten en cuenta que muchas billeteras web también están disponibles como aplicaciones móviles.

- **Billeteras web**

Puedes utilizar billeteras web para acceder a las blockchains a través de la interfaz de un navegador sin tener que descargar o instalar software en tu dispositivo. Esto incluye tanto a billeteras de exchange como otros proveedores de billeteras basados en navegador.



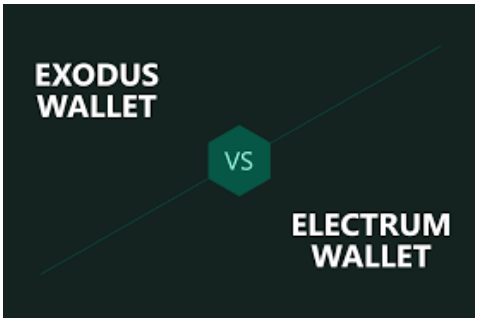
- **Billeteras de escritorio**

Como su nombre indica, las billeteras de escritorio son aplicaciones de software que los usuarios descargan y ejecutan localmente en sus computadoras. A diferencia de algunas versiones basadas en la web, las billeteras de escritorio proporcionan un control total sobre las claves y los fondos.

Cuando se crea una nueva billetera de escritorio, se crea un archivo llamado "wallet.dat" que se almacena localmente en una computadora. Este archivo contiene la información de la clave privada utilizada para acceder a las direcciones de las criptomonedas, cifrada con una contraseña personal[48].

Si proteges tu billetera de escritorio con encriptación, tendrás que introducir tu contraseña cada vez que ejecutes el software para leer el archivo wallet.dat .

Si pierdes este archivo u olvidas tu contraseña, lo más probable es que pierdas el acceso a tus fondos.



[48] ibid

- **Billeteras móviles**

Las billeteras móviles funcionan de forma muy similar a las billeteras web y de escritorio, pero están diseñadas específicamente como aplicaciones para teléfonos inteligentes. Son muy prácticas, ya que te permiten utilizar las criptomonedas estés donde estés. También puedes enviar y recibir activos digitales utilizando códigos QR.

Las billeteras móviles son ideales para realizar transacciones y pagos diarios, lo que las convierte en una opción viable para gastar Bitcoin, BNB y otras criptomonedas en el mundo real.

MetaMask, Trust Wallet y Phantom son ejemplos populares de billeteras móviles.

Sin embargo, al igual que las computadoras, los dispositivos móviles son vulnerables a aplicaciones maliciosas e infecciones de malware. Es una buena idea proteger tu billetera móvil con encriptación y una contraseña. Asegúrate de hacer una copia de seguridad de tu frase de recuperación (o claves privadas) por si pierdes el acceso a tu teléfono.

- **Billeteras impresas**

Una billetera impresa es un trozo de papel en el que están impresas físicamente una dirección de criptomonedas y su clave privada. Estas billeteras son muy resistentes a los ataques de hackers en línea y pueden considerarse una alternativa al almacenamiento en frío. Sin embargo, deben manipularse con cuidado y almacenarse de forma segura para evitar que se pierdan o se dañen.

1. **Regresando al ejemplo para A pueda realizar una transacción a B necesita primeramente que ambos tengan una cuenta en el mundo cripto, esta cuenta se denomina** BILLETERA O WALLET.

Entonces cuando un usuario crea una billetera lo primero que se configura es la clave privada y después de la generación de la clave privada, se procede a la creación de la clave pública, que es la que en su momento se va a compartir para realizar alguna transacción con otro usuario, la cual está relacionada matemáticamente con la primera, todo esto se logra con la aplicación de algoritmos seguros.

Regresando al ejemplo tenemos:

- **"A"** que tiene una billetera creada en BINANCE quiere realizar una transacción en criptomoneda, es decir enviara dinero a "B" porque está comprando un apartamento, y lo primero que hace es hacerlo saber a la red a la que está conectada,

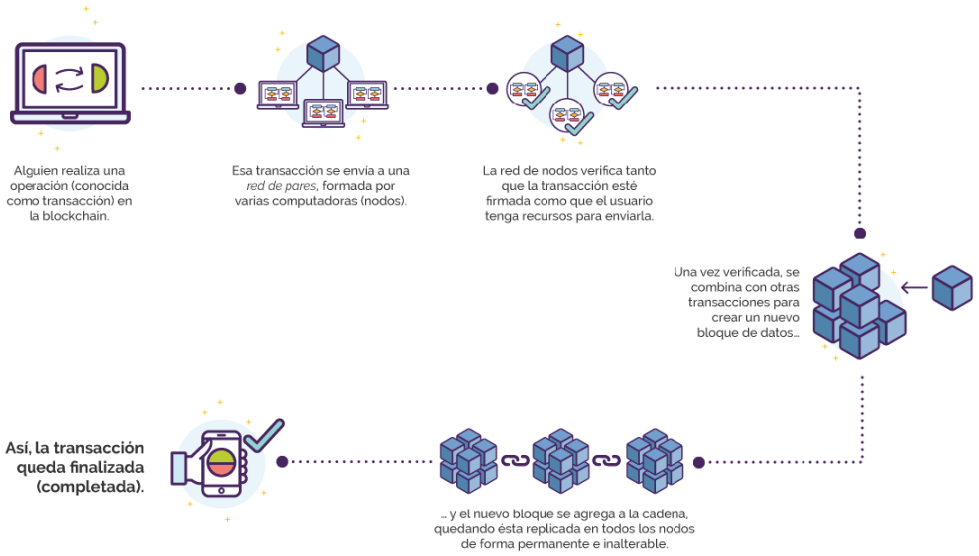
esta red está conformada por nodos, es decir usuarios conectados que se encargan de verificar la transacción, es decir verificar que:

- **A** tenga fondos para lo que desea enviar y si esto es así proceden a registrarlas en el gigantesco libro de cuentas denominado Blockchain.

- Para realizar la transacción **B** enviara su clave publica a **A** la cual se generará y como es Bitcoin la criptomoneda que tiene **B**, entonces esta dirección se vería así "**bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf3q5"** (esto es lo que recibiría **A** para enviar el Bitcoin)

- **A** por su parte ingresara esta dirección en su billetera y colocara la cantidad de Bitcoin que enviara a **B.**

- Una vez ingresada la dirección y cantidad esta transacción se realizará y quedará registrada en el famoso libro de cuentas denominado Blockchain y cualquiera que se conecte a la red podrá verificar dicha transacción, incluyendo a **A y B.**



Que concluimos de este proceso:

- Que las criptomonedas se emiten al margen de los gobiernos y bancos centrales y, al menos en teoría, esta función se traslada a todo aquel que quiera participar (los nodos o usuarios conectados que en su momento se convierten en validadores de las transacciones que se realizan).

- Que las criptomonedas, aunque lleven implícito la palabra moneda, y aunque las llamemos monedas digitales o virtuales, no son monedas, puesto que, para ser consideradas monedas deben de cumplir con al menos tres funciones básicas:

- Ser un medio de pago, para lo cual debería estar aceptadas de forma generalizada en la adquisición de bienes y servicios, con un fraccionamiento suficiente.

- Unidad de cuenta, porque podemos determinar el valor de cualquier producto en unidades de esta moneda

- Depósito de valor, manteniendo la capacidad de pago a lo largo del tiempo.

- Que en el proceso de transacciones existe un libro mayor público y descentralizado que registra todas las transacciones, garantizando la transparencia y la seguridad, denominado BLOCKCHAIN.

- Que no hay una entidad central que pueda determinar a ciencia cierta quien está detrás de la billetera de A y de la billetera de B.

2.6 Comercialización de los Criptoactivos

La primera transacción completada con bitcoin se produjo en mayo de 2010. Un programador compró dos pizzas y pagó por ellas 10.000 bitcoins, equivalentes entonces a 40 Dólares de Los Estados Unidos de América. Hoy equivaldrían a unos 90 millones de dólares[49].

De ahí en adelante utilizar criptoactivos para cualquier acto de comercio, se fue haciendo cada día una práctica más habitual.

Recordemos que todas estas modalidades de comercio de criptoactivos se llevan a cabo en la red, rara vez se establecerá contacto con la persona que esta atrás de cada dirección o billetera.

2.7 Como podemos utilizar los criptoactivos:

1. Plataformas de intercambio (Exchanges):

Los Exchange de criptomoneda es la plataforma en la que se realizan los intercambios de estas a dinero fíat o a otras criptomonedas. En estas casas de cambio online es donde se

[49] "Bit2me Academy: ¿Qué es un exchange de criptomonedas?",acceso 15 de mayo de 2025 https://academy.bit2me.com/que-es-exchange-criptomonedas/

genera el precio de mercado que finalmente marca el valor de las criptomonedas en base a la oferta y demanda.

Estas plataformas son el lugar principal para comprar, vender e intercambiar criptomonedas.

Existen exchanges centralizados (como Coinbase, Binance, Kraken) y descentralizados (DEX, como Uniswap)[50].

Exchanges centralizados: Esta categoría de exchanges incluye a las plataformas a la que los usuarios acceden para comprar o vender tokens según la cotización de los mercados. Suelen ser plataformas altamente reguladas, que cumplen con las normas de **KYC (Conoce a tu cliente) KYT** (conoce las transacciones) y **KYB** (Conoce el negocio) y **AML (Anti-Lavado de Dinero)**. Esto significa que no son plataformas privadas, pues el usuario debe dar a conocer su identidad para participar en la misma. Un ejemplo de estas plataformas puede ser **Binance**, **Kraken**, **Coinbase** o **Bitfinex**[51].

Los Exchanges descentralizados o DEX son una evolución directa de los exchanges tradicionales. Funcionan de forma muy parecida a estos últimos, pero cuentan con la capacidad de funcionar de forma descentralizada. Esto significa que no existen intermediarios y la plataforma se auto sustenta por su programación.

[50] Ibid
[51] Ibid

Además, los DEX suelen contar altos niveles de privacidad e incluso pueden llegar a ser anónimos.

2. Comercio entre pares (P2P):

Peer-to-Peer (P2P) significa literalmente de una persona a otra. Las redes P2P son aquellas redes de computadoras donde cada computadora actúa como cliente y como servidor.

Bajo esta modalidad puedes seleccionar tu precio de compra o venta de cualquier criptomoneda y encontrar a una persona dispuesta a realizar transacciones contigo a ese precio sin terceros centralizados que medien en la transacción. Sin embargo, existe un mediador descentralizado en forma de bolsa.

No hay cargos. Y como no hay intermediarios centralizados, tampoco hay comisiones. Además, no tienes que arriesgarte a perder tus fondos por culpa de un error de terceros.

Importante recalcar que todo este contacto se realiza en la red, no es de manera personal.

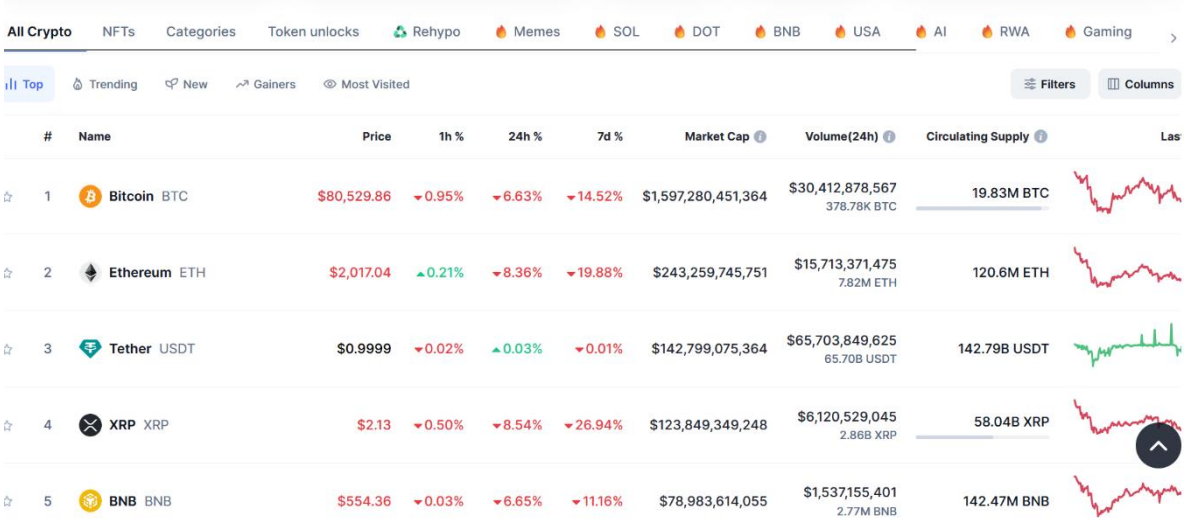
3. Pagos con criptomonedas:

Cada vez más negocios aceptan criptomonedas como forma de pago. Esto puede ocurrir a través de procesadores de pagos especializados o directamente entre billeteras digitales.

4. Inversión y trading:

El mercado de criptomonedas es un espacio libre para que cualquier persona invierta, buscando obtener ganancias a través de la compra y venta de activos.

El "trading" por su parte implica operaciones más frecuentes, buscando aprovechar las fluctuaciones del mercado.



Puntos importantes a considerar:

- **Volatilidad:** El valor de las criptomonedas puede fluctuar significativamente en cortos períodos de tiempo.
- **Seguridad:** Es crucial utilizar plataformas seguras y proteger las claves privadas de las billeteras digitales.
- **Regulación:** La regulación de los criptoactivos varía según el país, y está en constante evolución.
- **Información:** Antes de invertir o participar en el comercio de criptomonedas, es fundamental informarse adecuadamente.

2.8 Señales de alertas relacionados a la comercialización de criptoactivos

Las criptomonedas, por su naturaleza descentralizada y anónima, han creado un entorno propicio para que los estafadores diseñen y ejecuten esquemas fraudulentos como los esquemas Ponzi o Piramidal[52].

Respecto al uso de activos virtuales dentro de los cuales se encuentran las criptomonedas en esquemas de estafas y otros delitos, la Unidad de investigación Financiera

[52] "UIF. (s.f.). UIF: Obtenido de Unidad de Investigación Financiera, acceso el 15 de mayo de 2025, https://www.uif.gob.sv/

de la Fiscalía General de la República ha determinado una serie de señales de alerta y tipologías:[53]

- Empresas recién constituidas con registros altos en el volumen transaccional
- Renuencia del titular de la billetera para documentar transacciones y/o actualizar información
- Transaccionalidad con plataformas que tienen noticias negativas

Tipologías:

- Un cliente busca acceder a un crédito o a fondos propios, pero bajo alguna condición a plazo, y al cancelar su cláusula penal expresa que lo hace por una oportunidad de inversión cuyas condiciones de rentabilidad exceden irrazonablemente a las vigentes del mercado.

- **Retiro de fondos a wallet externas.**

Métodos utilizados:

1. Esquema Ponzi o Piramidal

Los esquemas de Ponzi conllevan programas de inversión falsos y no existentes en los que los inversores son víctimas de engaño al invertir, con la promesa de recibir un retorno inusualmente atractivo de su inversión. El operador o promotor del esquema mantiene la operación en funcionamiento pagando a los inversores iniciales con el dinero de los inversores

[53]" Grupo de Acción Financiera de Latinoamérica GAFILAT. (2024): Cuarta Actualización del Informe de Amenazas Regionales en materia de Lavado de Activos y Financiamiento del Terrorismo", acceso el 15 de mayo de 2025, https://campus.gafilat.org/login/index.php

nuevos hasta que el esquema se derrumba por su propio peso o el promotor desaparece con el dinero restante[54].

2. **Captación ilegal de fondos para realización de trading**

3. **Alto volumen de operaciones entre personas formando pequeñas redes de transacciones**.

Otras tipologías que pueden desarrollarse con el uso de criptoactivos son las siguientes:

Proyectos con "white papers" poco claros o plagio:

Un "white paper" es un documento técnico que describe el proyecto de criptomoneda. Es importante leerlo y entenderlo. Si es confuso, está incompleto, o detectas plagio, es una señal de alerta.

"Pump and dump" (inflar y vender):

Este esquema consiste en inflar artificialmente el precio de una criptomoneda para luego venderla masivamente, dejando a otros con pérdidas.

Uso de criptoactivos en la Dark Web

En la internet profunda (Deep web) los productos que se adquieren en los mercados clandestinos (armas, drogas, pornografía de menores, etc.) se pagan con criptomoneda, si bien

[54] Asociación de Especialistas Certificados en Antilavado de Dinero*, Guía de estudio Certificado de Especialista en prevención de blanqueo de capitales*. (EEUU, *ACAMS. 2024),*451

los delincuentes se están moviendo hacia Monero ya que el rastreo por parte de las fuerzas policiales en la práctica es imposible[55].

2.9 Debida Diligencia en la comercialización de criptoactivos

El comercio de criptoactivos ofrece diversas opciones, desde el intercambio en plataformas especializadas hasta el uso de criptomonedas como medio de pago. Sin embargo, es esencial tener en cuenta los riesgos y tomar precauciones para operar de manera segura.

Hay una variedad de formas en las que una institución, ya sea una institución financiera tradicional o una empresa criptográfica emergente, puede estar expuesta a la actividad relacionada con las criptomonedas y al riesgo que puede estar vinculado a esa actividad.

Algunos ejemplos incluyen:

- Instituciones financieras que buscan ofrecer todas las capacidades de comercio de criptomonedas y transferencia de activos.
- Negociación con fondos de liquidez
- Inversiones estratégicas en infraestructura blockchain
- Digitalizar/tokenizar tanto los productos tradicionales como la infraestructura que facilita el intercambio de esos activos.
- Acercando los servicios financieros tradicionales a las entidades vinculadas a las criptomonedas

[55]" TRM Labs: Explicacion de los mercados de la Darknet", acceso 15 de mayo de 2025, https://www.trmlabs.com/es/resources/blog/darknet-markets-explained

La debida diligencia del cliente es la base de cualquier programa sólido de cumplimiento de la normativa contra el LDA/FT/FPADM[56]. Conocer y comprender quiénes son los clientes determina el perfil de riesgo del cliente en el momento de la incorporación, cómo se le supervisa y la periodicidad en que debe actualizarse. En ese sentido cada actor vinculado al comercio de criptoactivos debe considerar cuidadosamente los elementos individuales del programa de Prevención de riesgos de Lavado de Dinero y activos, Financiamiento al Terrorismo, y Proliferación de armas de destrucción masiva, y los requisitos de control en función del tipo de negocio, la base de clientes y la oferta de productos.

Es por ello que, mediante la aplicación de un enfoque basado en riesgo (EBR), que consiste en identificar, evaluar y entender sus riesgos de LDA/FT/FPADM, le permitirá cada actor identificar la documentación idónea para asegurar que dichos riesgos se mitiguen eficazmente, y adoptar medidas proporcionales a los riesgos identificados; en ese sentido, cualquier órgano supervisor se encuentra limitado para dar una opinión relacionada a los procesos y catálogo de documentos que los sujetos obligados deben solicitar a la hora de iniciar o continuar relaciones comerciales con clientes, usuarios o contrapartes, por estar condicionado al nivel de riesgos que cada cliente en particular representa al sujeto obligado, debido a que los sistemas de prevención de LDA/FT/FPADM deben ser diseñados según las necesidades que cada sujeto obligado impone a partir de su estructura, actividad comercial, procesos o forma de constitución, apetito de riesgo, y lo laxo de estas dependerá de su línea de negocio.

De ahí que, la información solicitada a cada cliente debe ser definida por la institución financiera o cualquier empresa que se dedique al rubro y debe cumplir con el objetivo principal

[56] El comercio de criptoactivos ofrece diversas opciones, desde el intercambio en plataformas especializadas hasta el uso de criptomonedas como medio de pago. Sin embargo, es esencial tener en cuenta los riesgos y tomar precauciones para operar de manera segura.

que es identificar al cliente, entender su actividad económica esperada, las interacciones de la cuenta, la fuente y propiedad de los fondos, la naturaleza, el propósito y la utilidad que éste pretende darle a la relación comercial por entablar, evitando la aplicación de medidas excesivas.

No obstante, lo anterior, en el caso de los activos digitales, los sujetos que intervienen en el comercio de activos virtuales deben prestar singular interés en las interacciones actuales y futuras que el cliente espera tener en la cadena de bloques (Blockchain). Esto puede incluir la obtención y el análisis de las billeteras utilizadas por el cliente para comprender el riesgo histórico y la información transaccional del cliente y las interacciones con otros proveedores de activos virtuales, mediante el uso de la inteligencia y análisis de blockchain.

La inteligencia de blockchain proporciona a los usuarios la capacidad de evaluar la identidad de un cliente en función de su huella digital (es decir, la actividad que realiza en la cadena, cómo la realiza y con quién).

Algunos ejemplos incluyen:

- Reseñas de fuentes de fondos/fuentes de riqueza
- Facilitación de rampas de entrada y salida
- Selección de fondos de liquidez

Considerar utilizar los servicios de un proveedor de análisis de blockchain especializado, en este tipo de relación comercial es sustancial, en razón que, la inteligencia de blockchain proporciona a los usuarios la capacidad de evaluar la identidad de un cliente en

función de su huella digital, es decir, la actividad que realiza en la cadena bloques, cómo la realiza y con quién.

El monitoreo de transacciones también es una parte esencial en este tipo de relaciones para interrumpir el uso ilícito de instrumentos financieros. El monitoreo debe incluir evaluaciones generales de riesgo del perfil del cliente que brinden un panorama completo de la actividad, el comportamiento y con quién interactúa, a efecto de disponer de la información necesaria para evaluar de forma fiable el riesgo de la contraparte o cliente.

2.10 Entorno regulatorio de los Criptoactivos en el Salvador

El marco regulatorio de las criptomonedas en El Salvador se centra principalmente en la Ley Bitcoin, que hizo historia al convertir a Bitcoin en moneda de curso legal y posicionar al país como uno de los pioneros en la era del uso de criptoactivos.

Repasemos brevemente lo más destacado de cada normativa.

Ley Bitcoin:

Aprobada el 9 de junio de 2021, esta ley establece a Bitcoin como moneda de curso legal en El Salvador, junto con el dólar de Los Estados Unidos de América.

Otorga además al Bitcoin poder liberatorio irrestricto, lo que significa que puede ser utilizado en cualquier transacción, garantizando el estado la convertibilidad de Bitcoin a Dólar de Los Estados Unidos de América.

Ley de Creación del Fideicomiso Bitcoin[57]:

Esta ley establece el Fideicomiso Bitcoin, destinado a facilitar la convertibilidad de Bitcoin a dólares de Los Estados Unidos de América, es decir crear la infraestructura necesaria para la utilización del bitcoin, su objetivo principal es brindar confianza y estabilidad en el uso de Bitcoin como moneda de curso legal.

Nombre de la Ley, Norma o Instructivo	Vigencia	Contenido
NRP-29 Normas Técnicas para Facilitar la Participación de las Entidades Financieras en el Ecosistema Bitcoin	07/09/2021	Regulación de los sujetos que ofrezcan servicios basados en Bitcoin a sus clientes, ya sean personas naturales o jurídicas, y pudiendo estos servicios ser ofertados directamente o a través de un Proveedor de Servicios de Bitcoin
Lineamientos para la Autorización del Funcionamiento de la Plataforma Tecnológica de Servicios con Bitcoin y dólares	07/09/2021	Establecimiento de disposiciones aplicables para la autorización del funcionamiento de las plataformas tecnológicas de los servicios con Bitcoin y dólares de los Estados Unidos de América, que deseen proveer los sujetos obligados a sus clientes, sean estos personas naturales o jurídicas.
Decreto No. 27 – Reglamento de la Ley Bitcoin	26/08/2021	Desarrollar, facilitar y asegurar la aplicación de la Ley Bitcoin. El contenido está especialmente referido a la regulación del sistema bancario en el tema.
Ley de Creación del Fideicomiso de Bitcoin	30/08/2022	Constitución y regulación del funcionamiento del Fideicomiso Bitcoin. El Fideicomiso, en razón de que se constituye en favor del Estado y Gobierno de El Salvador, a través de los usuarios de la billetera digital estatal (wallet), se constituyó para un plazo indeterminado, a partir de la vigencia de esta ley.

Regulación de Proveedores de Servicios de Activos Virtuales (VASPs):

El Salvador también ha avanzado en la regulación de los proveedores de servicios de activos virtuales, siguiendo las recomendaciones del Grupo de Acción Financiera Internacional (GAFI).

En enero de 2023 entra en vigencia la Ley de Emisión de Activos Digitales (LEAD), permitiendo la tokenización de productos agrícolas (agro commodities), deudas y la emisión

[57] Ley de creación del Fideicomiso del Bitcoin, (El Salvador, Docuemntacion judicial, 2022), https://www.jurisprudencia.gob.sv/web/viewer.html?File=https%3A%2F%2Fwww.jurisprudencia.gob.sv%2FDocumentosBoveda%2FD%2F2%2F2020-2029%2F2021%2F08%2FE980A.PDF

de monedas estables como a USDT[58]. Esto permitió también la creación de un Registro de Proveedores de Servicios de Activos Virtuales (VASPs) que en un principio fue asumida por el Banco Central de Reserva en aquellos proveedores exclusivos de Bitcoin y la Comisión Nacional de Activos Virtuales para aquellos que involucraran otro tipo de criptomoneda; pero a través de las reformas a esta ley en agosto de 2024 se dispuso que ambos registros los debía asumir la comisión Nacional de Activos de Virtuales,

Lo relevante de estas normativas es que buscan fomentar la inclusión financiera y promover el uso de Bitcoin y otras criptoactivos en la economía salvadoreña, asimismo la Adopción de nuevas medidas y programas antilavado de activos, contra el financiamiento del terrorismo y contra la proliferación de armas de destrucción masiva para los Proveedores de Servicios Bitcoin y Proveedores de Activos Digitales.

[58] "Unidad de Investigación Financiera: «Estudio Estratégico Proveedores de Servicios de Activos Virtuales (PSAV)".» acceso el 15 de mayo de 2025, https://www.uif.gob.sv/

3 CAPITULO III

ANÁLISIS DEL TIPO PENAL DE ESTAFA INFORMÁTICA

SUMARIO: 3.1 Naturaleza del delito de Estafa Informática, 3.2 Definición del delito de estafa informática, 3.3 Elementos del Tipo Penal y 3.4 Tipos de Phishing, 3.5 Señales y Patrones reveladores del uso de inteligencia artificial en la comisión del delito de Estafa informática, 3.6 La causalidad lógica para establecer la imputación objetiva en el planteamiento de una teoría del caso para el delito de Estafa Informática

Este capítulo proporcionará un análisis legal exhaustivo de la estafa informática desde su naturaleza fundamental y definición hacia los elementos específicos requeridos para constituir el delito, asimismo profundizara en los métodos contemporáneos a través de los cuales se ejecuta la acción típica requerida es decir las metodologías vinculadas al uso de tecnologías de la información y comunicación.

3.1 Naturaleza del delito de Estafa informática

El surgimiento del delito de estafa informática tiene como fin crear una norma de control social tendiente a establecer y garantizar reglas básicas de convivencia, en el campo de las relaciones sociales patrimoniales que se desarrolla mediante la utilización de sistemas informáticos[59].

La Estafa Informática, es un delito autónomo respecto a la estafa simple, estamos acostumbrados a hablar del tipo penal básico de estafa, el cual difiere en gran medida de este tipo penal especial, ya que en aquel media una relación interpersonal entre estafador y víctima,

[59]Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos*, (, Granada, Editorial Comares 2002) 68.

en cambo en la estafa informática la conducta se lleva a cabo por el empleo de la manipulación informática o artificio semejante, consiguiendo de esta manera el sujeto activo la disposición patrimonial, el cual obtiene una transferencia no consentida por la víctima, y que en la mayoría de los casos no hay un contacto entre sujeto activo y víctima, es decir el delito de estafa informática carece de esa relación interpersonal.

¿Qué elementos vamos a encontrar en un delito de estafa informática?, bueno comenzaremos diciendo que va a existir una conducta fraudulenta, encaminada al uso indebido de elementos informáticos a través de la introducción o manipulación de datos falsos, que para llevar a cabo esta conducta se vuelve necesario hablar de componente físicos Hardware y lógicos del sistema informático (lenguaje informático, software).

Y por último debemos hablar de la finalidad del cometimiento de estos delitos, lo que se persigue es la obtención de un beneficio ilícito, ya sea en forma directa o indirecta y no siempre va a ser necesariamente patrimonial, aunque en la mayoría de los casos este perjuicio es meramente patrimonial.

3.2 Definición del delito de estafa informática

El tipo penal de ESTAFA INFORMATICA establece: *“ El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual*

procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco años."[60].

En el inciso segundo del referido artículo, establece que sancionará con prisión de cinco a ocho años[61], si las conductas descritas en el inciso anterior se cometieren bajo los siguientes presupuestos: a) En perjuicio de propiedades del Estado; b) Contra sistemas bancarios y entidades financieras, y se vieren o no afectados usuarios de los mismos; y, c) Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos.

Para comprender el contenido de este delito es preciso definir los componentes principales de su definición:

Las Tecnologías de la Información y la Comunicación: según la Ley Especial contra delitos Informáticos y Conexos, se refiere al "conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio,

[60] Ley Especial contra delitos Informáticos y Conexos. (El Salvador: Centro de Documentación Judicial, 2016) artículo 10.
[61] Ibid articulo 1

transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros[62].

Dato Informático: es cualquier representación de hechos, información o conceptos en un formato digital o análogos, que puedan ser almacenados, procesados o transmitidos en un sistema informático, cualquiera que sea su ubicación, así como las características y especificaciones que permiten describir, identificar, descubrir, valorar y administrar los datos,

Medio de Almacenamiento de Datos Informáticos: es cualquier dispositivo a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo;

Sistema Informático: es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información[63];

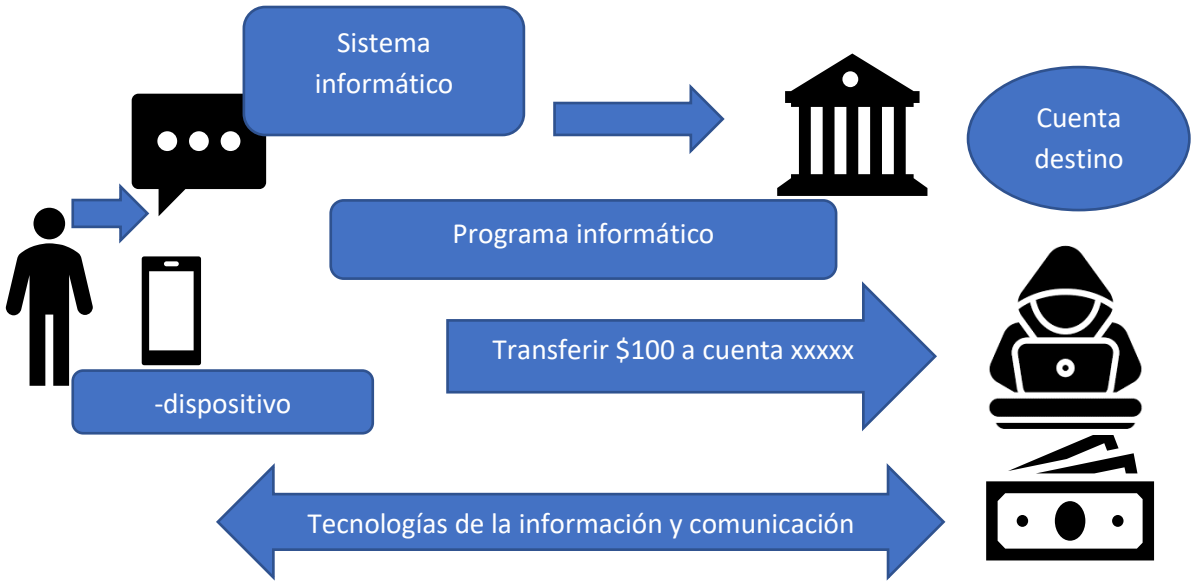
Sin el sistema operativo, el ordenador no es más que un elemento físico inerte. Todo sistema operativo contiene un supervisor, una biblioteca de programación, un cargador de aplicaciones y un gestor de ficheros. MS-DOS, Windows, Linux y Macintosh son los más conocidos, pero hay muchos más. Es un software que actúa de interfaz, entre los dispositivos de hardware y los programas usados por el usuario para manejar un computador. Es responsable de gestionar, coordinar las actividades y llevar a cabo el intercambio de los recursos y actúa como estación para las aplicaciones que se ejecutan en la máquina.

[62] Ibid
[63] Ibid

Dispositivo (Artificio Tecnológico): es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la Tecnología de la Información y la Comunicación.

Programa Informático: es la rutina o secuencia de instrucciones en un lenguaje informático determinado que se ejecuta en un sistema informático, pudiendo ser éste un ordenador, servidor o cualquier dispositivo, con el propósito que realice el procesamiento y comunicación de los datos informáticos.

Partiendo de estos elementos podemos aplicar los mismos a un caso práctico, a efecto de verificar la integración de todos los conceptos:



Como interactúan estos conceptos en la práctica, bueno en el entorno de las nuevas tecnologías de la información y comunicación que no es más que las herramientas y recursos tecnológicos que nos permiten comunicarnos, acceder a la información y realizar diversas tareas en la vida cotidiana,

encontramos la banca en línea de una institución bancaria x, que no es más que un software diseñado para realizar transacciones electrónicas, entendidas estas como aquella acción efectuada por una persona natural o jurídica denominada ordenante, a través de una entidad autorizada en la respectiva jurisdicción para realizar transferencias internacionales o locales, mediante movimientos electrónicos, con el fin de que una suma de dinero se ponga a disposición de una persona natural o jurídica denominada beneficiaria, en otra entidad o agencia autorizada para realizar este tipo de operaciones. El ordenante y el beneficiario pueden ser la misma persona.

Para llevar a cabo lo anterior se puede acceder desde cualquier dispositivo, que para el caso diagramado, del lado de la víctima un teléfono celular con un sistema operativo Android por ejemplo, y del lado del imputado una laptop con sistema operativo Android también, en esta interacción es claro que utilizando las nuevas tecnologías el imputado accede a la banca en línea de la víctima (esto como veremos más adelante inicia con la ingeniería social pero debe necesariamente realizarse una manipulación al sistema informático para accesar a la banca en línea de la víctima) e introduce las credenciales robadas y direcciona transferencias hacia su cuenta, que este proceso de introducir instrucciones al software de la banca en línea no es más que el uso del lenguaje computacional[64].

Partiendo de estos elementos que hemos obtenido de la definición legal del tipo penal se puede concluir lo siguiente:

[64] Superintendencia del Sistema Financiero: NRP-8 Normas Tecnicas para la gestión de los Riesgos de Lavado de dinero y Activos y de financiamiento al terrorismo, acceso 15 de mayo de 2025, https://ssf.gob.sv/images/stories/desc_normas_prud_bancos/NRP_08.pdf

- Como ya hemos acotado, un elemento diferenciador del tipo de estafa básico es la ausencia de engaño y error, por lo que en este caso la conducta típica se caracteriza por el hecho de que la disposición patrimonial se consigue valiéndose el autor de alguna "...operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema...".

- Respecto al acto de disposición patrimonial, es decir, la transferencia de activos patrimoniales, no consentida, se ha de entender el traspaso efectivo de un activo, es decir de un elemento patrimonial valorable económicamente, no es realizado por la víctima del engaño como en la estafa común, por la inexistencia del contacto humano, sino por el sujeto activo, habitualmente a través del sistema informático, que utiliza las Tecnologías de la Información y la Comunicación.

- No se enumeran específicamente los dispositivos que podrían ser considerados como sistemas informáticos o sistemas de información. En la mayoría de los contextos este enfoque se considera una buena práctica, en la medida en que mitiga el riesgo de que las nuevas tecnologías queden fuera de las disposiciones legales y de tener que actualizar constantemente la legislación. Con base en el concepto central del procesamiento de datos informáticos o información, es probable que las disposiciones apliquen normalmente a dispositivos como servidores y computadoras centrales, computadoras personales de escritorio, computadoras portátiles, teléfonos inteligentes, tabletas y computadoras de a bordo del transporte y la maquinaria, así como a los dispositivos multimedia como las impresoras, los reproductores de MP3, las cámaras digitales y las máquinas de juegos, por mostrar

ejemplos, de ahí que quede abierto a la inclusión de cualquier dispositivo que pueda existir a futuro.

3.3 Elementos del tipo penal

i) Bien Jurídico.

Según POLAINO El bien jurídico puede definirse como todo bien o valor normativamente evaluado y estimado como digno, merecedor y necesitado de la máxima protección jurídica. El bien jurídico puede ser de titularidad individual, (vida, integridad física) o colectiva (medio ambiente, salud pública, etcétera) y puede ser de carácter material (patrimonio, vida) o de naturaleza espiritual o inmaterial (honor, dignidad).[65]

Respecto al bien jurídico protegido, el tipo exige afectación del patrimonio económico del sujeto pasivo como la puesta en peligro de la seguridad de los datos informatizados y las funciones informáticas en sentido estricto.

Por lo que hay que precisar que el delito de Estafa informática se trata de un delito pluriofensivo, en tanto que la afectación se da en dos planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los bienes afectados a través de dicho sistema como lo es el patrimonio.

En primer lugar, el patrimonio, entendido por Salinas como "la situación de disponibilidad que tienen las personas sobre sus bienes, derechos o cualquier otro objeto,

[65] Polaino, Miguel Navarrete. *Lecciones de Derecho Pena Parte General,* (tomo II segunda edición corregida y actualizada. Editorial Tecnos, 2016) 156.

siempre que tal situación tenga una protección jurídica de relevancia económica"; debemos destacar que el patrimonio en este ilícito penal se encuentra representado, por ejemplo, a través de depósitos bancarios, fondos electrónicos, etc.

En segundo lugar, la integridad de los datos informáticos, por la cual se busca cautelar la inmutabilidad de los datos informáticos, lo cual implica la no alteración o modificación de las representaciones de hechos, información o conceptos expresados de cualquier manera que se preste a tratamiento informático, incluyéndose los programas diseñados para que un sistema informático ejecute una función.

En tercer lugar, la integridad de los sistemas informáticos, el cual, debe ser entendido como la no alteración o modificación de todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa, de esta forma este tipo penal también busca preservar la invariabilidad de los datos informáticos o de los sistemas informáticos éstos mediante algún empleo indebido de los mismos.

Sobre la información automatizada esta debe entenderse como el contenido de las bases y bancos de datos de los procesos informáticos, por lo tanto, se constituye un bien autónomo de valor económico. Y es la importancia del valor económico de la información lo que ha hecho que se incorpore como bien jurídico tutelado. Es decir, la información es un bien jurídico, que puede considerarse como de interés colectivo tutelado penalmente de forma conjunta con bienes de los particulares, siendo ambos de carácter homogéneo por lo que hay una relación mediana entre el derecho a la información como bien colectivo y los derechos

individuales que pueden verse afectados. El primero es medio o paso previo necesario para la lesión o puesta en peligro del segundo.

ii) Elementos objetivos

Pertenecen al aspecto objetivo: el sujeto activo, pasivo, la acción por el medio informático, el resultado producido mediante el fraude, y la relación de causalidad. Mediante que los elementos objetivos o descriptivos del tipo son: estados y procesos externos, susceptibles de ser determinados espacial y temporalmente, perceptibles por los sentidos (objetivos), fijados en la ley por el legislador en forma descriptiva.

a) Sujeto activo

El sujeto activo este revestido de una característica de Universalidad es decir cualquier persona natural que realice la acción propia del tipo penal, puede ser el sujeto activo del delito, sin que este requiera alguna calificación particular o especial o poseer específicos conocimientos técnicos en materia informática. Esto implica que el perfil del delincuente informático es muy amplio abarcando desde usuarios comunes hasta expertos en tecnología.

No se excluye como sujeto activo al titular legítimo del sistema al momento de efectuar una manipulación informática a su favor y en perjuicio de otro.

Es importante mencionar que otra característica del sujeto activo es la distancia y anonimato, la naturaleza de los delitos informáticos permite que los delincuentes operen desde ubicaciones remotas, lo que dificulta su localización y reduce su riesgo, esto es entendible dado que el uso de las nuevas tecnologías permite el acceso remoto desde cualquier parte de mundo.

Las implicaciones que esto tiene es que puede darse una diversidad de posibles sujetos activos y la dificultad para localizarlos plantea desafíos para la investigación y persecución de estos delitos, dado que como mencionaremos más adelante, en la mayoría de los casos se captura a las mulas financieras y no al sujeto que realiza la manipulación del sistema informático quien al final de cuentas es el destino final de los fondos que se transfieren, y que normalmente se encuentra en una jurisdicción diferente a donde se ejecuta la acción criminal.

Formas de ejecución y participación.

El delito de estafa informática es un ilícito de resultado material; al desvalor de acto debe agregarse el desvalor de resultado, es decir requiere para su configuración un perjuicio ajeno, a través del desplazamiento patrimonial no consentido, el cual fue logrado insertando instrucciones falsas o fraudulentas valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, la consumación del delito se logra en el momento de materializarse o lograrse, por parte del sujeto activo, la transferencia o desplazamiento patrimonial, siempre que ésta suponga un perjuicio para otra persona, natural o jurídica, ajena al autor del delito.

La participación en el delito de estafa informática es observable o imputable tanto en la calidad de autor, coautor, cómplice o cooperador e instigador.

Dentro de la anatomía del delito de informático es posible distinguir las siguientes modalidades delictivas[66]:

[66] Juan Manuel Sarrabayrouse, *Delincuencia Informática Patrimonial.* (Ediar, 2023)72

1. **La ingeniería social**-a través del uso de las nuevas tecnologías (ransonware (virus), phishing (farming, virus maliciosos) se tiene acceso a usuario-contraseña de la víctima, de su banca en línea-logrando así la manipulación del sistema informático.

Tendemos a vincular al sujeto activos de estos delitos como los famosos hackers-experto en descubrir vulnerabilidades de sistemas informáticos, cuando en realidad el ciber delincuente no necesariamente es un hacker, son personas comunes y corrientes con conocimientos básicos sobre informática con una intención especifica un ánimo de lucro-para si o para un tercero.

El reclutador y organizador de las mulas informáticas: Estas personas actúan como intermediarios entre los cibercriminales y aquellos que, a menudo sin saberlo, se convierten en instrumentos para cometer delitos informáticos, identifica personas para que presten sus cuentas o consigue las tarjetas inteligentes hurtándolas y utiliza las mismas para dicho fin.

Los muleros informáticos: una mula financiera es una persona que, a sabiendas o no, permite que otros utilicen su cuenta bancaria para transferir dinero obtenido de forma ilícita.

Se trata de la persona que recibiría en su cuenta el dinero obtenido de la víctima de la estafa, dificultando, de esta manera, el descubrimiento de los criminales. Si el mulero conoce que el dinero que recibe proviene de una estafa y forma parte por tanto de la organización del delito, será condenado como coautor o como cooperador necesario de un delito de estafa. Sin embargo, en la mayoría de las ocasiones no es así. En ocasiones los muleros son a su vez captados por las organizaciones criminales con engaños, como una oferta de trabajo con apariencia más o menos real, aunque con unas condiciones muy sugerentes, en la que se le dice

al sujeto que, a cambio de una cantidad o un porcentaje, debe abrir una cuenta a su nombre, recibir una transferencia de dinero y reenviarlo después a los estafadores.

b) Sujeto Pasivo

Los sujetos pasivos del delito son además del titular del derecho patrimonial objeto de afectación, los titulares individuales de la información, de los datos o programas objeto de la acción delictual, y de los equipos y sistemas afectados, aunque no sufran perjuicio económico patrimonial efectivo, así como la sociedad en general en cuanto titular de la información informatizada y de los sistemas por los que se procesa y transfiere. Esto es, solo pueden ser sujetos pasivos de este tipo penal las personas que, por una parte, sean titulares del bien jurídico patrimonio económico perjudicado y de los datos informatizados con valor contable y, por la otra, aquella persona que sea el titular del medio informático que resulta objeto de manipulación por parte del autor, que incluso puede ser una persona jurídica (instituciones crediticias, gobiernos, empresas, entre otros) que utilizan sistemas automatizados de información, generalmente conectados a otros.

c) Conducta típica

Se consuma ejecutando las siguientes formas de acción en un sistema que utilice las Tecnologías de la Información y la Comunicación:

El primer elemento de la conducta típica es la Manipulación: o influencia en el ingreso de los datos, según el autor Mata Martin en su obra delincuencia informática y derecho penal, esta fase previa en su ejecución práctica tiene un carácter previo puede ser activa en sentido estricto, modificando datos reales o añadiendo otros datos ficticios. En este caso los

datos tratados automáticamente son incorrectos, manteniéndose intacto el programa y siendo correcto el tratamiento o procesamiento de datos.

Para la realización de esta conducta el sujeto activo deberá valerse del uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta con la cual produce u obtenga un beneficio patrimonial indebido para sí o para otro.

El segundo elemento de la conducta típica es la transferencia no consentida de activos patrimoniales en perjuicio de tercero.

Contrariamente a la disposición patrimonial realizada por persona humana en el delito de estafa simple, en este caso se hace referencia a la transferencia realizada por una maquina sin intervención humana, dicha actividad es definida por la ley 53-07 sobre crímenes y delitos de alta tecnología de República Dominicana como "...toda transferencia de fondos iniciada a través de un dispositivo electrónico informático o de otra naturaleza que ordena instruye o autoriza a un depositario o institucional financiera a transferir cierta suma a una cuenta determinada...".

Dicha definición está inmersa en la exposición del término de la manipulación informática o artificio tecnológico, que sustituye el engaño que se da en la estafa común y recae sobre la máquina, siendo esta la que en virtud de dicha maquinación efectúa la operación de transferencia requerida por el estafador, puesto que la persona física no se encuentra en la posición de querer y poder realizar ese desplazamiento patrimonial, realizándolo el sujeto perpetrador por medio de la manipulación informática.

La transferencia no consentida de activos patrimoniales es consecuencia de la acción de manipulación, de la cual resulta la consiguiente disminución del patrimonio de un tercero. Por lo tanto, no tiene cabida la disposición inducida por error en una persona humana en detrimento de su propio patrimonio, sino, la transferencia realizada por una máquina sin intervención de persona humana.

Para que el delito se consume es necesario entonces que la manipulación a los sistemas informáticos produzca el resultado de una "transferencia de activos patrimoniales, entendida esta como el traspaso o cambio de titularidad de un valor patrimonial de cualquier naturaleza.

Este traspaso o cambio de titularidad de los valores patrimoniales debe además realizarse sin el consentimiento de la víctima que es el sujeto titular de estos, al consentimiento de este sujeto es al que se hace referencia, no así del titular del sistema que se manipula (como el banco, o la entidad a la que pertenezca el sistema informático), porque de no darse estas condicionantes, estaríamos en presencia de otros tipos penales, son así del delito de estafa informática.

Generalmente los elementos de la conducta típica se engloban un conjunto de acciones caracterizadas por el uso de programas, software, técnicas informáticas que permiten el acceso y manipulación de datos del sistema, y así ejecutar las acciones tendientes a obtener el beneficio económico.

La doctrina y la legislación comparada han identificado diversas modalidades de conducta que configuran el tipo de estafa informática en sentido técnico. Las principales son:

- ***Manipulación del input (datos de entrada)***

Esta modalidad consiste en la introducción de datos falsos o fraudulentos en un sistema informático para que éste procese operaciones que de otro modo no realizaría. El ejemplo más paradigmático es la introducción de órdenes de transferencia bancaria fraudulentas en los sistemas de un banco: el autor introduce datos falsos (una orden de transferencia desde una cuenta ajena) para que el sistema bancario ejecute una transferencia no autorizada. No hay ninguna persona que sea 'engañada': el sistema recibe los datos de entrada y los procesa conforme a sus algoritmos. El perjuicio se produce directamente como consecuencia del procesamiento automatizado.

- ***Manipulación del programa o del algoritmo de procesamiento***

Esta modalidad consiste en alterar los programas o algoritmos que determinan cómo el sistema procesa la información, con el fin de producir resultados patrimonialmente favorables para el autor. El caso clásico de la doctrina estadounidense —el llamado 'salami slicing'— ilustra esta modalidad: el programador bancario que modifica el algoritmo de redondeo de los intereses para que los céntimos o fracciones de centavo que resultan del redondeo sean transferidos a una cuenta de su titularidad, en lugar de ser absorbidos por el banco o sumados a las cuentas de los clientes. En cada transacción individual el perjuicio es ínfimo e imperceptible, pero la acumulación de millones de transacciones genera un perjuicio patrimonial significativo.

- ***Manipulación del output (datos de salida)***

Esta modalidad, menos frecuente pero igualmente constitutiva del tipo, consiste en la alteración de los datos que el sistema produce como resultado de su procesamiento, para hacer aparecer un estado patrimonial diferente del real. La falsificación del resultado de un proceso

de liquidación de haberes, por ejemplo, o la alteración de los estados de cuenta que el sistema bancario genera para sus clientes.

- ***Acceso no autorizado seguido de disposición patrimonial automatizada***

Esta modalidad combina el acceso ilícito al sistema con la manipulación posterior para producir el resultado patrimonial. El autor obtiene, por cualquier medio, las credenciales de acceso a un sistema bancario, fintech o de pagos electrónicos, y las utiliza para efectuar transferencias o pagos no autorizados. Esta modalidad es la más frecuente en la práctica y la que con mayor regularidad es incorrectamente calificada por los tribunales.

Importa destacar que en esta modalidad la distinción entre estafa informática y estafa simple depende de la forma en que el autor obtuvo las credenciales de acceso y de la forma en que el perjuicio se produce. Si el autor obtuvo las credenciales mediante un engaño dirigido a la víctima (phishing clásico: el autor envía un correo fraudulento, la víctima cree que es genuino, introduce sus credenciales en una página falsa y el autor las captura) y posteriormente utiliza esas credenciales para efectuar transferencias, la conducta tiene una doble naturaleza: el phishing es un delito ciberfacilitado (engaño interpersonal a través de medios tecnológicos) y el uso posterior de las credenciales puede configurar la estafa informática. Si, en cambio, las credenciales fueron obtenidas mediante un ataque técnico sin intervención humana de la víctima (keylogger, interceptación de comunicaciones, explotación de vulnerabilidades), todo el proceso es ciberdependiente.

- **Malware o Software malicioso:**

Este término es utilizado para referirse al software o programa de cómputo que son introducidos en los sistemas de información de los usuarios para causarles algún daño o

simplemente para modificar su uso y obtener su control. Siendo una de las funciones principales del malware que el ciberdelincuente, puede obtener el control y el acceso remoto al sistema de cómputos, y así poder grabar y enviar información y datos de los distintos usuarios a terceras personas sin tener conocimiento ni consentimiento alguno de los mismos, de esta manera se rastrean los hábitos de una persona en internet y todos los portales que visitan pudiendo transmitir a una fuente central[67].

Podemos hablar en forma variada de distintos tipos de software malware, como son en forma genérica los llamados virus como gusanos, troyanos, puerta trasera spyware, keyloggers, etcétera.

- **Spyware (programa espía)**

Estos son conocidos como archivos espías, spyware, mediante los cuales se logra la obtención de datos para suplantar a una víctima, reemplazando su personalidad para utilizar un servicio con alguna naturaleza económica, así, por ejemplo, tenemos las claves bancarias o de otro tipo de acceso, como son los números de tarjetas de créditos u otros similares. Al obtener la fórmula de acceso, estos mismos son posteriormente utilizados para recaudar y obtener alguna ventaja económica. Esa forma de obtención de clave se realiza ingresando al sistema operativo del ordenador de la víctima. Nos encontramos con una forma de obtención de clave usando la propia red, y por supuesto no teniendo autorización del titular o también teniendo

[67] Denominación genérica para hablar o referirse a cualquier tipo de programa o archivo dañino para el ordenador. Existen otras formas de descargas en los ordenadores, de todos estos programas como seria en el caso de la aparición en la pantalla, de una determinada página web la cual informa o da a conocer a los usuarios del sistema futuros premios o advertencia de detección de virus, o asimismo advertencia de alguna situación

acceso a la información en forma material es decir sustrayendo físicamente los mismos números o claves de acceso.

La manera que se obtienen de las claves puede ser muy variadas, ya sea en forma remota ingresando a un ordenador, puesto que se utiliza su IP para ello, o simplemente introduciendo en dicho ordenador estos archivos espías, para que posteriormente se puedan enviar al delincuente de la red los datos informáticos del sistema donde los han instalado, logrando con ello poder acceder al ordenador de la víctima. Podemos señalar entonces, que a través de estos softwares espías, que pueden ser instalados en los ordenadores múltiples programas, para tener el conocimiento de las claves o números de acceso, los cuales incluso pueden ser activados por la propia víctima, a través de ciertos controladores activex. En definitiva, estos softwares espías tienen la capacidad de auto instalarse en los ordenadores personales de los usuarios, con el objeto de conocer su identidad monitoreando el comportamiento de la persona al utilizar los distintos sistemas o navegar por internet, estos softwares al igual que las *cookies*, son capaces de crear bases de datos y proporcionar la información correspondiente, esto lo hacen a base de las distintas preferencias o hábitos de los usuarios. Al respecto se puede citar a Steven Gibson, quien descubrió algunos mecanismos espías en una gran cantidad de programas software, todos ellos utilizados tanto por los gobiernos, las empresas y las personas, afirmando que, en un ordenador personal, es muy altamente probable que contenga algunos programas espías escondidos en sí mismo, puesto que en el mundo existen millones de archivos espías instalados, sin que sepan las personas.

- **Troyanos**

Es un software dañino disfrazado de software legítimo. Un programa caballo de Troya es capaz de replicarse por sí mismo y por tanto, son aplicados con cualquier tipo de software por un programador o puede contaminarlo el equipo por medio del engaño. Debe su nombre al hecho histórico en el cual los griegos invadieron la ciudad de Troya, utilizando el engaño, mediante un caballo de madera, donde en su interior ingresaron los griegos para invadir dicha ciudad. Estos programas encubiertos, parecen que fueran útiles, pero, sin embargo, ellos ocultan un código para ejecutar acciones indeseables sobre el ordenador, activándose cuando el usuario utiliza la aplicación, que piensa o cree que es útil.

- **Puerta trasera**

Se han denominado puerta trasera o en inglés *backdoor,* un software que tiene la particularidad, que permite a quien conoce el funcionamiento, el acceso al sistema del ordenador, poder saltar los métodos usuales de auténtica aplicación, con algún fin delictivo. Estos programas son incluidos deliberadamente para uso legítimo, también son un riesgo para la seguridad, ya que cualquier persona que la descubre pues era sistema en el que están ejecutando.

- **Redes zombies**

Cuando hablamos de zombies, identificamos a los ordenadores que de alguna manera es infectado por algún tipo de malware, las formas de infección pueden ser muchas pero normalmente es una puerta trasera, entrada que ha sido encontrada por la vulnerabilidad del ordenador del usuario. Al hablar de red zombies, consecuentemente con el fraude no ha sido autorizado por el usuario del ordenador correspondiente, hablando en términos de secuestro del equipo.

En este caso lo primero que hace es el delincuente informático, toma la máquina, arma una red de miles de PCs, y después analiza cuál es el uso que le dará. Al hablar de botnets[68] (anglicismo que se refiere a la asociación en red), hablamos de máquinas autónomas, puesto que ellos concentran un gran número de máquinas zombies que se coordinan, pudiendo usar todas ellas una vez tomadas y en un segundo inundar miles de casillas de correo con spam. También pueden alojar, en los ordenadores, sitios de phishing, o páginas de pornografía, igualmente pueden sustraer información, y propagar malware, pudiendo en la misma red ir variando el delito. Un dato necesario es que la red botnets, se venden o se rematan en foros de hackers

- **keyloggers (registrador de teclas)**

O también registro de tecleo, es otras de las formas que se hace necesario mencionar y que comúnmente se encuentra en los denominados cibercafé, son los llamados *keyloggers*[69] (vendría siendo un programa malvare), que tienen como fin registrar todo lo que la persona digite en el teclado, pudiendo con ello posteriormente el ciberdelincuente, acceder a las claves abriendo dichos programas.

Es un tipo especial de software espía o spyware, instalándose comúnmente junto a otros que prometen mejorar de alguna forma el ordenador.

[68] "RedFoundation, The Shadowserver: The Shadowserver Foundation. s.f." acceso el 15 de mayo de 2025, https://www.shadowserver.org/topics/botnets/

[69] "KEYLOGGER POR HARDWARE: Definición de Keylogger (registrador de pulsaciones de teclas)" acceso 12 de Junio de 2023, https://www.alegsa.com.ar/Dic/keylogger.php#gsc.tab=0

- **Bombas lógicas y bombas de tiempo**

Son programas que se ejecutan en unos momentos específicos o cuando o existen condiciones óptimas para ejecutarlos, utilizando una rutina programada posterior a su instalación, esperando circunstancias apropiadas de tiempo, de fecha, de realización de algún pago etc. en este caso es necesario realizar una determinada conducta, como sería por ejemplo digitar una palabra determinada o cierta combinación en las teclas para que se active, o también ejecutan un programa especial.

Son programas altamente destructivos, creado para ser ejecutados en determinado tiempo incluso a cierta hora del día, y que son capaces de destruir e inutilizar equipos, redes y servidores tanto física como lógicamente.

- **Camaleón**

Son similares a los virus troyanos, siendo programas malignos disfrazados como otros programas generalmente enviados por correo electrónico, actuando como un programa similar a otro que sea de confianza del usuario, pero con la diferencia que produce inmediatamente los daños, no basándose en un programa que ya existe en el ordenador del usuario, sino que diseña otro completamente nuevo, utilizándose en aplicaciones concretas, y no en programas comerciales. Es decir, estos imitan fielmente el programa que reproducen. Un programa de tipo camaleón dañino, se puede utilizar como, por ejemplo, con el fin de derivar dinero de una cuenta a otra, a través de una transacción bancaria, pero utilizando la técnica del centavo, es decir poco a poco sin que el usuario se dé cuenta van sustrayendo dinero, con este programa similar al real.

- **Especial referencia al Phishing (cosecha y pesca de contraseñas)**

El Tribunal Supremo Español *ha definido al phishing* como el correo recibido, que proviene de grupos organizados que utilizaban la red informática para la captación de los datos confidenciales de los titulares de las cuentas, y consistente en envío masivo de correos electrónicos que simulan proceder de entidades bancarias, cuyo mensaje imita exactamente el diseño, logotipo, firma, utilizado por la entidad bancaria para comunicarse con sus clientes, y a través de los cuales obtienen datos personales que, al ser introducidos en la página falsa, son captados para ser utilizados de forma fraudulenta. En dichos correos se apremia al internauta a actualizar datos personales, como nombres de usuarios y contraseña de motivos de seguridad, mantenimiento, mejora en el servicio, etc., redirigiéndoles a una página que imita a la original e introduciendo sus datos en dicha página falsa, lo que permite a los autores de la misma tomar los datos y utilizarlos de forma fraudulenta.

El *phishing o pesca de datos*, hoy por hoy es una de las técnicas más frecuentes usadas por los delincuentes informáticos. Dicho terminó proviene de las palabras del idioma inglés *password harvesting y fishing*, que en su conjunto sería *cosecha y pesca de contraseñas*, por ende, *pícher*, hace alució a la persona que realiza este tipo de acciones.

Desde los años 90 en adelante, se comenzó a utilizar esta técnica, la cual se centraba en el envío en gran cantidad de correos electrónicos con un contenido fraudulento, tanto a personas naturales como jurídicas, tomando el nombre de *smishing* o vishing según la modalidad cuando los mismos son remitidos, a través de mensajes o llamadas telefónicas. La información enviada al usuario va en directa relación con sus identidades en línea y con las credenciales de acceso que la persona utiliza parta acceder a la red, *logins y passwords* de mensajería instantánea, también claves ingresar a sus perfiles que activados en las redes sociales o las contraseñas de sus correos electrónicos. Las técnicas del *phisher* han ido variando

en el tiempo y no sólo se limitan a ser aplicadas en menajes telefónicos, sino que también en la colocación de post en Facebook o Twitter, en los cuales se trata de motivar a la víctima que ingrese por los beneficios que ello traerá, siempre y cuando se digite la información personal para posteriormente cometer la acción delictiva.

Esta técnica de captación ilícita de datos personales se basa en la confianza de las entidades suplantadas, pudiendo tener muchas variantes y métodos para usar, toda vez que, a través de *malware*, se puede lograr instalar programas maliciosos, como los ya estudiados (troyanos, gusanos, etc.) en el sistema donde la víctima tiene sus diversas claves de acceso.

El phishing se ha convertido en una de las técnicas más prevalentes en la comisión de estafas informáticas. Su efectividad radica en la capacidad de los ciberdelincuentes para manipular la confianza de las víctimas, suplantando la identidad de entidades legítimas. A través de correos electrónicos, mensajes de texto o llamadas telefónicas fraudulentas, los estafadores inducen a las personas a revelar información confidencial, como contraseñas, datos bancarios o números de tarjetas de crédito. Esta información se utiliza posteriormente para realizar transacciones no autorizadas, robar identidades o acceder a cuentas personales, causando así un perjuicio económico a la víctima.

La Evolución del Phishing y su Impacto en la Estafa:

Con el avance de la tecnología, las técnicas de phishing se han vuelto cada vez más sofisticadas. Los ataques ya no se limitan a correos electrónicos genéricos y mal redactados, sino que incluyen mensajes altamente personalizados y convincentes, diseñados para engañar incluso a los usuarios más precavidos. Además, el phishing se ha diversificado, extendiéndose a plataformas de redes sociales, aplicaciones de mensajería y otros canales de comunicación

digital. Esta evolución ha incrementado significativamente el número de víctimas de estafas informáticas, generando pérdidas millonarias y afectando la confianza en las transacciones en línea.

Aspectos Legales y Desafíos:

Desde el punto de vista legal, el phishing se considera un delito de estafa informática, ya que implica el uso de engaño y manipulación para obtener un beneficio económico ilícito. Sin embargo, la persecución de estos delitos presenta desafíos significativos debido a la naturaleza transfronteriza de internet y la dificultad para identificar a los responsables. La cooperación internacional y la actualización constante de las leyes son fundamentales para combatir eficazmente el phishing y proteger a los usuarios de las estafas informáticas.

3.4 Tipos de Phishing

1. Phishing Tradicional

En esta modalidad, el fraude es más simple, desde el punto de vista técnico, porqué está vinculado a una simple copia de un sitio, que es familiar para la víctima, en el cual se reemplaza la dirección del mismo, dirección a la cual llegan los datos ingresados por el usuario, momento en el cual las claves de ingresadas pueden estar en algún archivo de texto o ser enviadas algún correo electrónico. La diferencia con los otros, que está vinculado solamente a un sitio web, donde en el cual se instalan los contenidos de la página emulada.

2. Phishing redirector

En este caso, estilizado a través de correos electrónicos masivos, que se basan en que a pesar de que son pocos los usuarios comprometidos o las víctimas afectadas, igualmente se comete el fraude. Esta modalidad requiere que el delincuente informático, realice un mayor esfuerzo técnico para crear las páginas falsas, en este caso se crean dos o más sitios o dominios para realizar el fraude[70].

3. **Spear phishing**

Esta forma de ataque tiene la característica que va dirigido a un cierto número de personas, se utiliza la ingeniería social y un estudio previo complejo de las víctimas, es decir son métodos personificados y a la vez con un alto porcentaje resultado delictivo.

En este caso no buscan que sea algo masivo, sino que apunta a determinados perfiles de usuarios, donde se envían correos electrónicos con todos los datos para que la víctima crea, que es un correo verdadero, se van creando todo un escenario de direcciones conocidas, para generar en la persona la confianza que se necesita para ingresar los datos necesarios. En este caso el delincuente cibernético, busca el eslabón más débil dentro de la institución que quiere defraudar, buscando siempre personas que no estén vinculadas a la informática, para así lograr su cometido.

4. Smishing SMS

Mediante el smishing SMS, se utilizan el servicio relacionado con el canal digital, como son los teléfonos celulares. Mediante ellos los usuarios de telefonía móvil recibe mensajes

[70] ESET - Christian Ali. Spearphishing: Correos con asunto 'Nuevo Voicemail' intentan robar credenciales corporativas., acceso el 06 de Febrero de 2025, https://www.welivesecurity.com/es/phishing/spearphishing-nuevo-voicemail-robo-credenciales-outlook/

donde se falsifica los sitios y vínculos de portales para sustraer información personal del usuario, comúnmente entregando algún tipo de código o número especial para validar algún premio. Lo que se busca con ello es la ganancia económica, que puede revestir múltiples formas de estafa. Hoy en día también se utiliza, las aplicaciones como son Telegram o WhatsApp, aprovechando que en estas nuevas aplicaciones de comunicación, no es necesario algún pago para enviar el mensaje respectivo, sólo es necesario estar conectado a Internet.

5. Vishing

Esta es una técnica reciente que está basada en la telefonía que utiliza el protocolo IP, en la cual se envía mensajes de correo imitando el nombre marca alguna intrusión bancaria o de pago, le indican a la persona que marque un número determinado de teléfono, respondiéndole un sistema automatizado donde contestan solicitando información personal. Estos falsos centros de detención telefónica, en ocasiones están vinculados a otro, de tal forma que se complementan para dar mayor veracidad a la llamada respectiva confines de engaño, teniendo mayor efectividad.

- **Pharming308 (granja de servidores o DNS)**

El pharming es una modalidad en la cual el delincuente informático desvía el tráfico de internet de un sitio web hacia otro con apariencia semejante309. Esta modalidad se considera una variante del phishing, en la cual se manipula las direcciones DNS310[71], que utiliza el usuario. Esto se realiza, modificando un archivo llamado Hosts, que puede encontrarse en cualquier ordenador que funcione bajo Windows, y que además utilice internet explores, de esta manera el usuario digital su navegador la dirección de la página a la que quiere acceder, y

[71] [71]"Activate 2016: Extracto de curso realizado en Google, acceso 15 de mayo de 2025, http://google.es/activate

es reenviado a otra creada por el defraudador que tiene el mismo aspecto que la original, ingresando los datos necesarios sin que se percate, que dicha página no es la verdadera. Lo más reciente en esta modalidad, se trata que para no ser descubierto, se envía un enlace en el correo electrónico remitido, por la supuesta entidad financiera en el cual va un archivo adjunto HTML para que el destinatario lo descargue, así ocultando su verdadera URL. Así las cosas, una vez que la víctima ha picado, descarga y abre el archivo que contiene un formulario que recoge los datos, el delincuente ingresa al sistema informático de la entidad bancaria, pudiendo disponer de la cuenta.

Esta técnica tiene su fundamento en los ordenadores que se encuentren conectados a Internet y tienen una dirección IP única. Las URLs, sólo direcciones que se utilizan para localizar los recursos en Internet, esta misma se compone de varias partes, (protocolo de acceso o de comunicación, el nombre de dominio, que puede contener en su dominio, la ruta al documento y el documento el dominio es un hombre único que normalmente se emplea para identificar un sitio web en internet, hoy en día se ha introducido el nombre de dominio internacionalizado, por ello es posible utilizar nombres de dominio con caracteres en otros idiomas[72].

De esta manera, aunque se pueda identificar un ordenador por su nombre de dominio, en realidad internamente en internet identifican los ordenadores por medio de la dirección IP, es decir cualquier dispositivo que se conecta a Internet, ya sea un ordenador, una tableta, un teléfono móvil tiene asignada una dirección IP. El nombre de dominio va asociados a la dirección IP, algo así como un número telefónico y la dirección de una casa. Cuando se utiliza

[72]"Activate 2016: Extracto de curso realizado en Google, acceso 15 de mayo de 2025, http://google.es/activate

el pharming, se ataca, ya sea directamente a un ordenador específico o directamente a los servidores DNS, donde varios usuarios se verían afectados.

- **Técnica del salami (cortado en rodajas, salami)**

Consiste en la sustracción o desvío de pequeñas cantidades de activos de un número importante de cuentas a la del sujeto activo. Toma su nombre, toda vez que la técnica utilizada o patrón comisivo, es través del minucioso o porcionado en rodajas, hace alusión a las láminas muy delgadas al cortar un embutido, en este caso son múltiples y pequeñas porciones de dinero que se traspasan a la cuenta del delincuente, todo lo cual se aprovecha del redondeo de intereses[73].

En el ámbito de las estafas informáticas, la técnica del salami se manifiesta de diversas maneras, todas caracterizadas por la extracción gradual y encubierta de pequeñas cantidades de dinero o información, que en conjunto suman un gran perjuicio. Aquí algunos ejemplos:

- **Desvío de pequeñas cantidades en transacciones masivas:**

Los estafadores pueden manipular sistemas informáticos para desviar fracciones de centavos o pequeñas cantidades de dinero de un gran número de transacciones. Estas cantidades, individualmente insignificantes, se acumulan en una cuenta controlada por el delincuente, generando un beneficio considerable.

- **Manipulación de redondeo en sistemas financieros:**

[73] MIRIAN HERRERA Moreno.”Revista de Actualidad Penal, número 39.”El fraude informático en el derecho penal español. (Sevilla, 2001) 938.

Se puede modificar el código de programas de cálculo de intereses o comisiones para que el redondeo siempre favorezca al estafador. Al aplicar esta manipulación a un gran volumen de transacciones, se logra desviar pequeñas sumas de dinero de cada cliente, que se acumulan en un monto significativo.

- **Robo de pequeñas cantidades de datos personales:**

En lugar de realizar un robo masivo de datos, los estafadores pueden extraer pequeñas porciones de información personal de diversas fuentes. Estos datos, combinados, permiten construir perfiles completos que se utilizan para el robo de identidad o la realización de fraudes.

- **Ataques a cajeros automáticos:**

Mediante virus informáticos, o manipulaciones informáticas, se puede lograr que de miles de cajeros automáticos se extraigan pequeñas cantidades de efectivo, dificultando enormemente su detección.

La técnica del salami en las estafas informáticas se aprovecha de la capacidad de la tecnología para realizar pequeñas manipulaciones a gran escala, logrando un beneficio ilícito considerable de forma silenciosa y difícil de detectar.

- **3.5 Señales y Patrones reveladores del uso de inteligencia artificial en la comisión del delito de Estafa informática.**

Definir la IA no es fácil, ya que el concepto de inteligencia per se no es del todo preciso; La inteligencia artificial (IA) es la rama de las ciencias computacionales que se encarga del diseño y construcción de sistemas capaces de realizar tareas asociadas con la inteligencia

humana[74], coloquialmente podemos decir que la inteligencia artificial se usa cuando una máquina es capaz de imitar las funciones cognitivas propias de la mente humana, como: creatividad, sensibilidad, aprendizaje, entendimiento, percepción del ambiente y uso del lenguaje.

Sus aplicaciones van desde el reconocimiento en imágenes o video de objetos y personas, hasta el habla y la traducción automática de textos, pasando por el diagnóstico y tratamiento de enfermedades y la toma de decisiones; el uso de la inteligencia artificial en el dio día en los diferentes campos de aplicación, ha llegado hasta el sector financiero, en el cual se utiliza para el reconocimiento de patrones de fraudes y lavado de dinero y acticos en los miles de transacciones que se realizan a diario en las entidades financieras, permitiendo detectar señales de alerta y patrones claves en la actividad criminal.

Pero por otro lado la inteligencia artificial (IA) ha transformado el panorama de los delitos informáticos, permitiendo a los delincuentes crear estafas más sofisticadas y difíciles de detectar. A continuación, mencionara algunas de las señales y patrones reveladores que pueden indicar el uso de IA en la comisión de estos delitos.

- Phishing hiper-personalizado: Los correos electrónicos o mensajes de phishing generados por IA pueden imitar el estilo de escritura de remitentes conocidos, contener detalles específicos sobre la víctima (obtenidos de redes sociales u otras fuentes) y ser extremadamente convincentes.

[74] "Foro consultivo científico y tecnológico: inteligencia artificial", acceso 15 de junio de 2025, https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf

Dado que el salir a pescar a gran escala tenia como limite la capacidad humana, ahora bien a través de la inteligencia artificial se pueden crear campañas masivas con un alto grado de personalización, algo que antes era inviable humanamente.

- **Ingeniería social mejorada:** La IA puede analizar grandes volúmenes de datos para crear perfiles detallados de posibles víctimas, lo que permite a los estafadores diseñar ataques de ingeniería social altamente dirigidos y efectivos, explotando vulnerabilidades emocionales o psicológicas.

- **Suplantación de identidad avanzada (Deepfakes y clonación de voz)**

Deepfakes de voz: La IA puede clonar voces con una precisión asombrosa, lo que permite a los estafadores suplantar la identidad de familiares, ejecutivos de empresas o figuras de autoridad en llamadas telefónicas para solicitar transferencias de dinero o información confidencial.

- **Deepfakes de video e imagen**: Se utilizan para crear videos o imágenes falsas pero realistas de personas, que pueden usarse para estafas de criptomonedas, suplantación de CEO, o para difamar y extorsionar.

- **Identidades sintéticas:** La IA permite crear identidades falsas, generando información personal, fotografías y documentos realistas que se utilizan para abrir cuentas fraudulentas o realizar transacciones no autorizadas.

Con esta técnica tiene a través de ingeniería social diversa información que las personas suministran a través de redes sociales y combinan estos datos reales de información con información fabricada nombres inventados direcciones falsas números de teléfono inexistentes turno el objetivo de construir perfiles que a primera vista apadicen a auténticos y con estos realizar la actividad criminal ya me dice que pasemos pero fíjate despacho entonces

- **Automatización y escalabilidad de ataques:**

Bots y agentes de IA: Los ciberdelincuentes utilizan la IA para automatizar la creación de perfiles falsos en redes sociales, enviar mensajes automatizados, gestionar múltiples perfiles en sitios de citas (estafas románticas) o crear chatbots de atención al cliente falsos para recopilar información[75].

Los bots son softwares desarrollados que permiten adivinar por ejemplo contraseñas partiendo del análisis de una gran cantidad de datos o lo que es igual que en una brecha cortísima de tiempo puede probar miles y miles de contraseñas hasta dar con la contraseña correcta para detectar la vulnerabilidad en un dispositivo esto lo pueden realizar en miles de cuenta a la vez, lo que permite acceder a un innumerable de cuentas de personas a la vez, lo cual permite que se desarrolle un fishing de una manera mucho más efectiva y más rápida que si detrás de esta técnica estuviera un ser humano.

[75]“ Universidad de Nebrija:introducción a la inteligencia artificial”, acceso 15 de junio de 2025, https://www.nebrija.es/~cmalagon/ia/transparencias/introduccion_IA.pdf

- **Malware avanzado**: La IA puede desarrollar malware que se auto-optimiza y evade la detección por parte de sistemas de seguridad tradicionales, alterando su código para no coincidir con firmas conocidas[76].

Con la IA es posible generar variantes de malware que cambian su código o estructura con cada infección a un dispositivo electrónico esto dificulta enormemente y la detención por parte de antivirus y la IA ayuda a detectar patrones en los sistemas de seguridad y mutar para evadirlos es decir mejorar las técnicas y pasar desapercibidos y detectar vulnerabilidades en diversos dispositivos electorales

- **Análisis de grandes volúmenes de datos:**

Relleno de credenciales y ataques de fuerza bruta: La IA puede analizar patrones en contraseñas y probar credenciales robadas en múltiples plataformas hasta encontrar una coincidencia, facilitando la toma de control de cuentas.[77]

La IA es capaz de guiar a un criminal paso a paso en un hackeo de un dispositivo electrónico, de direccionarlo y proporcionarle técnicas en busca de vulnerabilidades, básicamente el ciberdelincuente se acompaña de un guía paso a paso para lograr la manipulación de un sistema informático**.**

¿Como es posible reconocer estos patrones en el cometimiento del delito de estafa de informática?

[76] Ibid
[77] ibid

La clave para detectar el uso de IA en estafas informáticas radica en estar alerta a la sofisticación, la personalización inusual, la calidad de la suplantación de identidad (especialmente en voz y video), la automatización de las interacciones y cualquier comportamiento que parezca "demasiado bueno para ser verdad" o que genere una urgencia injustificada.

iii) Elemento subjetivo.

Es un delito doloso, compatible con el dolo directo y tal cual se establece en el Convenio de Budapest[78], se exige como parte del dolo la motivación especial del ánimo de lucro personal o para beneficio de un tercero.

Se establece por tanto la necesidad de que el sujeto activo haya actuado con la voluntad y el conocimiento de manipular un sistema informático o cualquiera de sus componentes, datos informáticos o información contenida en ellos, y logre insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita la transferencia no consentida de activos patrimoniales en perjuicio de tercero beneficio o provecho para sí o para un tercero.

Ánimo de lucro.

Está representado en el delito en comento, como la pretensión del sujeto activo en el sentido de obtener como resultado de la conducta típica, un provecho para sí o para un tercero en perjuicio ajeno; con base en lo anterior, se puede señalar que el momento en que se logra consumar el delito es cuando se materializa o consigue, por parte del sujeto activo, la transferencia o desplazamiento patrimonial, siempre que esta suponga un perjuicio para otra

[78] Europa, C. d. (2001). Convenio sobre la Ciberdelincuencia (Convenio de Budapest). Obtenido de https://www.coe.int/en/web/cybercrime/the-budapest-convention

persona, sea jurídica o física, ajena al autor del delito. Situación que se logra con la participación activa del sujeto receptor en sus cuentas del dinero en tanto el mismo permite de manera activa la disposición final del dinero, mediante el retiro del mismo de un cajero automático o institución bancaria o su transferencia a terceros nacionales o extranjeros.

3.6 La causalidad lógica para establecer la imputación objetiva en el planteamiento de una teoría del caso para el delito de Estafa Informática

En el planteamiento de una teoría del caso para el delito de estafa informática, la causalidad lógica para establecer la imputación objetiva es un elemento crucial y, a menudo, complejo. No basta con demostrar que una acción causó un resultado (causalidad naturalística); es necesario determinar si ese resultado puede ser atribuido objetivamente al autor desde un punto de vista jurídico-penal.

I. Causalidad Naturalística (o Nexo Causal)

Este es el primer paso y el más básico. Se pregunta si la conducta del acusado fue una condición sine qua non (una condición sin la cual el resultado no se hubiera producido) del perjuicio patrimonial.

En el delito de la estafa informática: Se debe demostrar que la "manipulación informática o artificio semejante" (la acción delictiva) fue el factor que llevó directamente a la "transferencia no consentida de cualquier activo patrimonial que para el caso particular se trata de criptoactivos".

Ejemplo: Si el ciberdelincuente insertó un código malicioso en un dispositivo electrónico para captar usuario y contraseña, ese código es la causa natural del desvío o transferencia de fondos que realiza posteriormente. Si envió un correo de phishing y la víctima hizo clic, ese clic fue la causa natural de la posterior transferencia.

¿Cómo opera la imputación objetiva?

Aquí es donde la causalidad lógica se vuelve fundamental. **La imputación objetiva va más allá del mero nexo causal y exige que se cumplan ciertos criterios para que el resultado pueda ser jurídicamente atribuido al autor. Los criterios principales son:**

i. Creación de un riesgo no permitido o jurídicamente desaprobado:
ii. La conducta del acusado debe haber generado un riesgo relevante y no tolerado socialmente para el bien jurídico protegido (el patrimonio, uso de datos en la estafa informática).

En el delito de la estafa informática: La manipulación del sistema informático o el artificio tecnológico utilizado con el fin de captar credenciales o cualquier dato o información de la víctima **no son riesgos permitidos**. Son, por definición, acciones diseñadas para alterar ilegítimamente el funcionamiento del sistema informático de un dispositivo electrónico que no es propiedad del ciberdelincuente, las TICS utilizadas no para sus función positiva sino por el contrario para procurar el cometimiento de un delito, y esto además se realiza con fines de lucro, lo que se persigue con la manipulación del sistema informático es transferir fondos hacia las cuentas de los ciberdelincuentes.

Veamos algunos ejemplos de la manipulación de dispositivos: Acceder sin autorización a una cuenta, modificar datos, introducir un virus, suplantar una identidad digital para obtener dinero, son todas conductas que crean un riesgo no permitido para el patrimonio ajeno.

Realización del riesgo en el resultado:

El resultado (la transferencia patrimonial no consentida y el perjuicio) debe ser la materialización directa de ese riesgo no permitido creado por la conducta del autor. No debe haber interrupciones o cursos causales atípicos que desvíen la cadena causal.

En la estafa informática: El perjuicio patrimonial debe ser consecuencia directa de la manipulación o artificio semejante, es decir si el ciberdelincuente modificó el algoritmo de un cajero automático para que entregara dinero extra y ese dinero fue retirado, el perjuicio es la realización del riesgo creado por la manipulación. Si se usó una identidad sintética para obtener un crédito, el impago y el perjuicio son la realización del riesgo de la creación fraudulenta de la identidad.

Ámbito de protección de la norma:

El resultado debe estar dentro del alcance o finalidad de protección de la norma penal (el tipo de estafa informática). Esto excluye aquellos resultados que, aunque causalmente conectados, no son los que la norma busca evitar.

En la estafa informática: El Art. 10 de la LEDIC busca proteger el patrimonio de las personas frente a manipulaciones o artificios tecnológicos que provoquen transferencias patrimoniales no consentidas. Si el resultado es la pérdida patrimonial por una de estas conductas, entonces está dentro del ámbito de protección.

Es importante recalcar la importante distinción con la estafa tradicional: A diferencia de la estafa común (Art. 215 CP), en la estafa informática no se exige el "engaño a la víctima" como elemento central, ni un "acto de disposición patrimonial consciente" por parte de la víctima. El elemento que sustituye el engaño es la "manipulación informática o artificio semejante", que actúa sobre el sistema automatizado. Esto es clave para la causalidad y la imputación, ya que el error lo sufre la máquina o el sistema, no una persona; esto porque como bien se dijo supra el sistema informático

o maquina cree que la persona que esta haciendo uso del mismo es el usuario, dado que está utilizando las credenciales del mismo, o esta realizando un artificio tal tecnológicamente hablando que da como resultado una transferencia de activos, que hace creer al sistema o maquina que es el usuario el que lo realiza cuando no es así.

Consideraciones especiales con el uso de IA:

Cuando se involucra la IA en la estafa informática, la complejidad de la causalidad lógica y la imputación objetiva puede aumentar:

- Identidades Sintéticas: Si se usa una identidad sintética generada por IA para obtener un crédito, la "manipulación" no es sobre un sistema en un único acto, sino la construcción y el "cultivo" de una identidad falsa que lleva al perjuicio. La causalidad se establece en la cadena de eventos que culmina en la aprobación fraudulenta del crédito. El riesgo creado es la existencia de una "persona" fraudulenta con la capacidad de obtener beneficios financieros.
- Malware con IA: Si un malware auto-modificable y evasivo (impulsado por IA) causa un perjuicio, la imputación sigue siendo al autor que creó y/o distribuyó ese malware, porque su acción inicial fue la que creó el riesgo no permitido que se materializó en el resultado.

- Automatización: La automatización de ataques mediante bots (muchos de ellos con IA) no rompe la causalidad ni la imputación objetiva. La acción original de programar o lanzar los bots es la que genera el riesgo, y el resultado es la materialización de ese riesgo a través de los medios automatizados.

En síntesis, la causalidad lógica en la imputación objetiva para la estafa informática se centra en demostrar que la manipulación o artificio tecnológico del autor fue el factor determinante y jurídicamente desaprobado que generó y materializó un riesgo ilícito en el patrimonio de la víctima, resultando en la transferencia no consentida de activos y el consecuente perjuicio, todo ello con ánimo de lucro; no debemos olvidar que en el delito informático en la mayoría de los casos son estructuras criminales las que ejecutan el delito, y ahí es preciso valorar la coautoría y distribución de roles justamente para no romper el nexo lógico causal. La intervención de la IA no altera estos principios fundamentales, pero puede hacer más compleja la fase de prueba al difuminar las líneas de la acción humana directa en la comisión del delito.

4. CAPÍTULO IV

LA EVIDENCIA DIGITAL EN EL DELITO DE ESTAFA INFORMÁTICA

SUMARIO: 4.1 Definición de prueba electrónica o digital, 4.2 características de la evidencia digital, tipología de la prueba electrónica, 4.3 la pericia informática, 4.4 Agente encubierto digital como técnicas de investigación informática especializada.

Se ha venido hablando en los capítulos que preceden que, las modalidades delictivas han evolucionado a una velocidad vertiginosa a la par de las nuevas tecnologías. Se ha enmarcado al delito de estafa informática, como un delito que se aprovecha de la infraestructura tecnológica y la confianza de los usuarios en el entorno digital. No importa cuál sea la modalidad que utilicen para accesar o manipular los sistemas o programas informáticos, desde el phishing sofisticado hasta el acceso indebido a datos bancarios y las transacciones fraudulentas en línea, los perpetradores dejan tras de sí un rastro invisible pero potencialmente revelador: la prueba digital.

Este capítulo se adentra en el crucial papel que desempeña la prueba digital en la investigación y el enjuiciamiento del delito de estafa informática. A diferencia de los delitos tradicionales, donde la evidencia física puede ser tangible y directa, la estafa en el ciberespacio se caracteriza por su naturaleza intangible y transfronteriza.

La prueba digital, que abarca desde registros de comunicaciones a través de las diversas plataformas de redes sociales y direcciones IP hasta metadatos de archivos y logs de actividad, se erige como la piedra angular para reconstruir los hechos, identificar y localizar a los responsables y demostrar su culpabilidad en un proceso judicial.

La correcta identificación, recolección, preservación y análisis de la prueba digital se ha convertido en habilidades esenciales para los investigadores y profesionales del derecho que se enfrentan a la creciente complejidad del delito de estafa informática. Este capítulo explorará las diversas formas que puede adoptar la prueba digital en este contexto, los desafíos inherentes a su manejo y las mejores prácticas para garantizar su validez y admisibilidad en un proceso judicial.

4.1 Definición de Prueba electrónica o Digital

Hablar de prueba nos direcciona necesariamente a hablar del derecho de prueba, concebido este como un derecho fundamental dentro del debido proceso legal que garantiza a las partes en un procedimiento judicial la oportunidad de presentar las pruebas que consideren pertinentes para sustentar sus alegaciones o defensas.

Es definido también como *"aquel derecho fundamental, de configuración legal, que asiste a cualesquiera partes (activas o pasivas), en cualesquiera tipos de procesos (penales y no penales), y por medio del cual aquellas ostentan el derecho a proponer los medios de prueba que consideren pertinentes para acreditar los hechos en que se fundamenten sus respectivas pretensiones, el derecho a que sean admitidas judicialmente las pruebas que resulten pertinentes y útiles, y el derecho a que las inadmitidas lo sean por resolución judicial motivada, así como, por último, el derecho a que las pruebas admitidas sean efectivamente practicadas o ejecutadas"*[79].

Este derecho tiene diversas manifestaciones:

[79] Jose Garberi LLobregat. *Constitución y Derecho Procesal. Los fundamentos constitucionales del Derecho Procesal.* (Madrid: Civitas-Thomson Reuters, 2009) 265.

1. El derecho a proponer los medios de prueba que cada parte procesal considere adecuados para acreditar los hechos en que fundamenten sus respectivas pretensiones[80].

Ahora bien, esta proposición de los medios de prueba autorizados por el ordenamiento deberá hacerse dentro de los plazos previstos y de la forma legalmente predeterminada, es decir, en la forma y momento establecidos legalmente.

2. El derecho a que sean admitidos por el tribunal que esté conociendo de proceso todos aquellos medios de prueba propuestos por las partes que, a juicio de aquel, se manifiesten pertinentes y útiles[81].

Esto implica que cumpliendo los requisitos formales para el ofrecimiento de prueba y en aras del principio de libertad probatoria, cumplidos estos presupuestos, los medios de prueba deberán ser admitidos para su producción en el momento procesal oportuno.

3. El derecho a que las pruebas inadmitidas lo sean mediante resolución judicial motivada en su impertinencia o en su inutilidad[82].

Ello implica que el rechazo que carezca de motivación, vulneraría este derecho, pues se trataría de un rechazo arbitrario o improcedente.

[80] Ibid
[81] Ibid. 266.
[82] Ibid

4. El derecho a que sean practicadas las pruebas que hayan sido admitidas judicialmente por haber sido consideradas pertinentes y útiles, las cuales habrán de ser llevadas a la práctica sin desconocimiento ni obstáculo[83].

En resumen, el derecho de prueba asegura que las partes tengan la oportunidad de presentar su versión de los hechos (la teoría fáctica) y los elementos que la respaldan ante un tribunal imparcial, permitiendo así que la decisión judicial se base en la totalidad de la información relevante disponible.

Es importante destacar que este derecho no es absoluto y que el mismo está sujeto limitaciones establecidas por la ley, **como la pertinencia, la legalidad y la utilidad de la prueba**. Además, el tribunal competente tiene la facultad de rechazar pruebas que considere irrelevantes, inadmisibles o dilatorias.

De igual manera la proposición de prueba está sujeta a los plazos previstos y de la forma legalmente predeterminada por ordenamiento jurídico determinado, para nuestro caso en particular, el Código Procesal Penal.

Una vez que se ha delimitado el derecho de prueba es necesario definir que debemos entender por "prueba", siguiendo a Parajeles Vindas, el término "prueba" alude, desde un punto de vista técnico, "…*a la actividad de las partes encaminadas a convencer al juez de la veracidad de unos hechos que se afirman existentes en la realidad*"[84].

Por su parte, Antillón considera que la prueba puede definirse "…*como el conjunto de juicios de hechos formados en la mente del juez (convicción), en función de contraste-*

[83] Ibid 263
[84] Ibid.

*corroboración de los juicios de hecho formulados por las partes como fundamento de sus pretensione*s"[85].

La primera definición se enfoca en la actividad de las partes para presentar la información al juez. La segunda definición se enfoca en la reacción del juez a esa información, cómo la procesa y cómo forma su propia comprensión de los hechos.

Ambas definiciones son complementarias. Las partes realizan una actividad probatoria con la intención de generar una convicción en el juez. El juez, a su vez, evalúa esa actividad a través del contraste y la corroboración para formar su propio juicio sobre los hechos. La prueba, por lo tanto, es el puente entre las afirmaciones de las partes y la convicción del juez, siendo fundamental para la correcta administración de justicia.

Ahora bien, es preciso centrarnos no en todos los medios de prueba sino en la **prueba digital o electrónica**, definida esta como ***"la información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para formar la convicción en torno a una afirmación relevante para el proceso. Una fotografía, un video, una página web, un correo electrónico, una base de datos, una contabilidad en un programa de cálculo Excel –por citar algunos ejemplos–, en cualquier soporte (digital, magnético o informático), constituyen una 'prueba electrónica' […], aun cuando su reproducción e impugnación puedan ser diferentes"[86].***

Asimismo, se observa que la prueba electrónica puede ser ***objeto* o *medio de prueba***. La prueba electrónica puede ser objeto de prueba, y así se habla de probar un hecho electrónico

[85] Ibíd
[86] Xavier Abel Lluch, *Derecho probatorio*, (J.M. Bosch Editor, España, 2012.)928

(por ejemplo, el envío de un correo electrónico en determinada fecha). Puede ser un medio de prueba, y así se alude a probar electrónicamente un hecho (por ejemplo, un correo electrónico en el que el demandado reconoce expresamente una factura pendiente pago). O puede, simultáneamente, **ser objeto y medio de prueba**, cuando se trata de probar electrónicamente un hecho electrónico (por ejemplo, la celebración de un contrato a partir de los correos electrónicos enviados desde las terminales de dos ordenadores)[87].

Es claro que la inclusión de la prueba digital o electrónica es una manifestación directa del principio de libertad probatoria aunado a la evolución y desarrollo de las nuevas tecnologías, este sentido, en este capítulo desarrollaremos el tratamiento probatorio de aquellas fuentes de prueba en las cuales interviene necesariamente algún dispositivo electrónico sea para su creación, almacenamiento o reproducción.

4.2 Características de la evidencia digital

Las singularidades inherentes a la evidencia digital subrayan la necesidad de que los investigadores y profesionales de la informática forense diseñen y apliquen técnicas especializadas, además de adherirse a procedimientos rigurosos para salvaguardar estas características[88].

Características	Descripción
Volatilidad	Los datos digitales pueden cambiar o desaparecer rápidamente si no se manejan rápidamente

[87] Ibíd

[88] Miriam Gerardine Aldana de Lara, Sandra Luz Chicas, Glenda Yamileth Baires, Samuel Aliven Lizama, Carlos Javier Rosa Monterrosa, y José Miguel Alas Alfaro. «*Guia sobre evidencia digital en la legislación salvadoreña/* (El Salvador, segunda edición, 2024)

Fragilidad	Susceptibilidad a alteraciones o destrucción por errores en la recopilación.
Persistencia	Capacidad de ser recuperados incluso después de eliminados o modificados
Múltiples copias	Datos replicados en varias ubicaciones para análisis forense sin alteraciones.
Aislamiento	Separación de la evidencia para prevenir cambios durante la investigación.
Dinamismo	Cambios continuos que afectan la recolección y análisis de la evidencia.
Redundancia	Información disponible en múltiples ubicaciones, requiere gestión cuidadosa.
Trazabilidad	Metadatos registran información de creación modificación y acceso de archivos
Intangibilidad	Naturaleza electrónica que necesita herramientas especializadas para análisis
Complejidad Técnica	Requiere alto conocimiento de sistemas y datos para análisis forense.

4.3 Tipología de la prueba electrónica.

Es posible distinguir cuatro bloques de pruebas considerada electrónica o digital, sin el ánimo que las misma se consideren numerus clausus::

1. En un primer bloque podríamos ubicar a las pruebas electrónicas creadas directamente a través de la informática, es decir, todas aquellas informaciones que no disponen de un formato físico, o que originariamente nacen de la informática como algo intangible y pueden ser pasadas a un formato físico[89].

Aquí encontraríamos, sobre todo, correos electrónicos, archivos informáticos, *cookies*, sitios de rastreo de historial informático, *webs*, comentarios vertidos en *chats*, foros o redes sociales como *Facebook* o *Twitter.*

2. En un segundo bloque encontraríamos las pruebas electrónicas que proceden de medios de reproducción o de archivos electrónicos, videos o fotografía digital

Aquí podríamos ubicar a los archivos, fotos o video procedentes de cámaras digitales, videocámaras o *smartphones*[90].

3. En el tercer bloque podemos incluir las pruebas electrónicas que se presentan mediante un *hardware* propiamente informático y que tienen una naturaleza propiamente y puramente electrónica[91].

[89] Leo Bladimir Benavides. *La Prueba Electrónica*. *Breves acotaciones sobre el documento electrónico*. Acceso 15 de mayo de 2025, https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/4/2010-2019/2018/03/C94AC.PDF
[90] Ibid
[91] Ibid

En este bloque encontraríamos instrumentos como un CPU, un disco duro externo, un pendrive –"memoria USB", en El Salvador– o cualquier dispositivo instalable por medio de una conexión USB u otro puerto similar. Aunque realmente estos son soportes y no debemos confundirlos con la prueba en sí que serían los datos que están dentro, existen casos específicos en los que tendrían validez como prueba en sí.

4. En el cuarto bloque es posible situar una serie de pruebas mixtas: las pruebas tradicionales entrarían en contacto con las nuevas tecnologías de la información, con lo que estaríamos en presencia de pruebas modificadas[92].

Aquí podríamos señalar la prueba pericial informática, que es la prueba destinada a examinar y valorar las pruebas contenidas en los tres bloques antes mencionados y que necesita de profesionales capacitados; asimismo podemos mencionar las declaraciones de parte o interrogatorios de testigos que se efectúen a través de sistemas de videoconferencia; entre otras.

4.4 Partiendo de esta clasificación podemos entrar a analizar los más relevantes:

- **Correo electrónico**

Esta compuesto del contenido del mensaje junto a sus anexos (texto, imagen, vídeo) y de los datos de tráfico (fecha, hora, duración, origen y destino)[93].

La acreditación de un *mail* puede efectuarse mediante cualquiera de los dispositivos electrónicos de remisión o recepción, y/o en cualquiera de los servidores implicados, resultará

[92] Ibid

[93]Teresa Armenta Deu. «*Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre de 2018*, (Revista Internet derecho y politia, IDPM dosier implicaciones jurídicas, 2018.)

más sencillo probar el contenido del mensaje mediante el acceso a los dispositivos electrónicos utilizados para la comunicación por el emisor o el receptor del mail.

El acceso puede darse en una fase administrativa (investigación a cargo de un agente fiscal) o en una fase judicial (procesos judicializados bajo la jurisdicción y control de un juez), y mediante dos vías, provocada o voluntaria; la elección dependerá de la utilización que las partes pretendan darle, en razón que la utilidad del contenido puede ser utilizado para robustecer la tesis fiscal o fundamentar la defensa de los imputados.

En un acceso voluntario, el interesado en utilizar la información deberá proporcionar el usuario y contraseña para ingresar al correo electrónico ya sea en un dispositivo (table, computadora, Tablet, celular, etc) o en la nube, mediante la navegación en internet. En ambos casos, deben considerarse la opción de correo electrónicos eliminados como una forma suprimir evidencia.

El acceso provocado, usualmente, se solicita en procesos judicializados y recae sobre aparatos electrónicos incautados previamente a los procesados. En ambos casos, la pericia debe realizarla un profesional en la materia, por lo que, para el nombramiento, acreditación, puntos de pericia, y presentación de informe debe sujetarse a las condiciones establecidas en el Art.226 y siguientes del código procesal penal.

La efectividad de la información obtenida por este medio dependerá del manejo de los aparatos electrónicos sobre los cuales recaerá la pericia, en razón que, los datos que se pretende obtener están disponibles en la nube y puede ser obtenidos y eliminados por cualquier persona que conozca usuario y contraseña de la cuenta de correo a la que se pretende acceder, es decir, si al aparato incautado no se le interrumpió el acceso a internet mediante la activación del modo

avión, el riesgo que no se encuentre la información es latente, no basta con el aseguramiento físico del dispositivo, evitar el acceso remoto es vital en este tipo de investigaciones.

En ambos casos, teniendo presente que afectará al derecho fundamental a la intimidad y/o al secreto de las comunicaciones, según el acceso al correo electrónico tenga lugar con anterioridad a iniciar el proceso de comunicación o no sea así, y según se trate de los datos de cabecera o el contenido del mensaje, **deberá solicitarse la autorización judicial para la extracción, fijación de imágenes y análisis de la información.**

Asimismo, su aportación al proceso será mediante un medio probatorio adecuado: en formato papel o como documento electrónico, a través de copia del disco duro o del disco duro del servidor al que llegó el correo electrónico, con su correspondiente *código hash,* acompañándose del correspondiente informe, cuyas conclusiones podrán incorporarse mediante prueba pericial.

- **Redes sociales y otros elementos web**

Del inabarcable mundo de las redes sociales me centraré en el hecho de que cada usuario construya un perfil público o semipúblico en un sistema delimitado o cerrado y en que se elabora una lista de otros usuarios que comparten relaciones, pudiendo recorrerse la lista de relaciones que las personas tienen con otras del sistema.

Entre las múltiples consecuencias jurídicas que implica este quehacer, presenta relevancia probatoria la información obtenida de las redes sociales y la prueba de los hechos delictivos cometidos en las mismas. En el primer sentido, la investigación de los hechos requerirá fuentes y medios clásicos y novedosos orientados a investigar la huella digital, la autoría y/o la localización de la empresa prestadora del servicio.

Por lo que se refiere a la información obtenida en las redes sociales, se orientará a analizar el rastro digital, tanto para investigar un ilícito cometido en la red como fuera de ellas. La titularidad de la cuenta puede ser también el objeto de investigación, lo que se hará averiguando la dirección IP utilizada para colgar el contenido ilícito y, a partir de ahí, la cesión de datos de identificación y localización del dispositivo, identificación que precisará de autorización judicial.

¿Cómo se obtiene esta información?

Las partes pueden proporcionar información contenida en las redes sociales, tanto de perfiles propios como ajenos a cuyo contenido se pueda acceder lícitamente, entregando el dispositivo mediante el cual han tenido contacto con el criminal.

En el caso de que se trate de perfiles sospechosos de cualquier red social, es preciso obtener en primer momento el **url o dirección del perfil sospechoso**, esto a través de entrevista con testigos, o por la entrega voluntaria del dispositivo involucrado, con esta información se procede a solicitar la autorización del acto urgente de investigación o como diligencia en el plazo de instrucción "Obtención y resguardo de información electrónica de la cuenta de Facebook…" Por ejemplo, esta autorización judicial permitirá que la entidad titular de la red social proporcione la información concerniente al perfil solicitado.

En relación a lo anterior, previo a la obtención y resguardo de información electrónica de un perfil de red social, el investigador (fiscal o policial) debe tomar en cuenta que el URL, Localizador de Recursos Uniforme (Uniform Resource Locator), es la dirección de una página web o archivo en internet, que permite a los usuarios localizar y acceder a recursos digitales, y que para el caso de redes sociales, la URL es la dirección web que dirige a los usuarios a un

perfil o página específica en una plataforma. A diferencia de las URL de sitios web generales que dirigen a diversos tipos de páginas web, las URL de redes sociales enlazan específicamente a páginas en redes sociales como LinkedIn, Twitter, Facebook, Instagram y otras. Verbigracia, la URL de una red social para el perfil de Facebook de una empresa podría verse así: https://www.facebook.com/FGR.SV/.

La importancia de la anterior aclaración en este tipo de investigaciones radica en que, si se cambia el nombre del perfil de la red social, también cambia el URL para el direccionamiento, y probablemente cuando el investigador necesite localizar y acceder al perfil o página específica en una plataforma ya no esté disponible porque ha cambiado su nombre o ha sido eliminada.

Para evitar lo anterior, el agente fiscal o policial, además de solicitar el **URL o dirección del perfil sospechoso o publicación**, debe solicitar el ID de la red social, ya que, este es un número único que identifica a un perfil, mientras que una URL es la dirección web que lleva a ese perfil, y mediante el ID la obtención y resguardo de información electrónica de la cuenta o perfil de la red social se podrá realizar aunque este haya sido eliminado o cambio su nombre, ya que este incluye, además del dominio de la plataforma, el identificador del perfil o página.

El servicio de obtención y resguardo de información electrónica de cuentas o perfiles de redes sociales está disponible en línea para las autoridades de orden público y se puede acceder desde las mismas plataformas de redes sociales previo cumplimiento de requisitos legales mínimos, como comprobar que pertenece a una institución de las fuerzas de la ley, FGR, PNC, CSJ, que la información será utilizadas en procesos investigativos activos y que se

cuenta con las facultades legales nacionales para realizar este tipo de requerimiento, lo cual se visualiza así:

Una vez recibida la respuesta del proveedor de servicios de la red social, el cual es remitido de forma expedita y por medios electrónico mediante correo electrónico, este informe contendrá información primordial que permitirá dar seguimiento a la investigación y en el mejor de los casos individualizar al responsable:

- Números telefónicos asociados al perfil
- Ips de conexión
- Correos electrónicos

Es importante mencionar que el periodo de resguardo de información electrónica de cuentas y perfiles de redes sociales tiene un periodo de 90 días, y en caso que se requiera un periodo mayor debe notificarse al proveedor de servicios quienes previo acceder a lo solicitado le exigirán una autorización judicial que justifique la prolongación del resguardo.

Vale aclarar que la información remitida, en un primer momento, solo puede ser utilizada como indicios de existencia y participación positiva, y no como prueba por la forma que es remitida. Para que revista los efectos probatorios exigidos por los estándares procesales salvadoreños debe iniciarse un Procedimiento de Asistencia Legal Mutua en Materia Penal, el cual inicialmente estaba conferido a la Corte Suprema de Justicia, artículo 182, numeral 3 de la Constitución de la República, pero desde el mes de enero de 2024, luego de las reformas realizadas al código procesal penal en el Decreto Legislativo No 929, de fecha 3 de enero de 2024, publicado en el Diario Oficial No 5, Tomo 442, de fecha 9 de enero de 2024, la autoridad central y competente para la asistencia mutua en materia penal es el Fiscal General de la República, por medio de la Unidad de Asuntos Legales Internacionales, Art. 502-JJ.- Código Procesal Penal.

WhatsApp y otros sistemas de mensajería instantánea.

Las especiales características de esta forma de comunicación entre usuarios mediante una aplicación para teléfonos móviles y *smartphones* que permite enviar mensajes de texto, notas de audio y vídeo, compartir contactos o la propia ubicación presentan algunas diferencias con el correo electrónico y SMS, ya que la información transmitida no se conserva por un servidor externo, se utilizan protocolos de seguridad para garantizar el cifrado de la información y resulta disponible en multiplataforma: IOS, Android, Windows Phone.

Para este caso en particular hay dos vías de actuación para obtener evidencia digital:

1. Primera: en el caso de que se trate del perfil sospechoso, se buscara la obtención de información del perfil involucrado, de la misma manera que ya se relacionó supra en el caso de redes sociales.

2. Segunda: Segunda: cuando se cuenta con dispositivos electrónicos que tienen instalada la aplicación en comento tales como Tablet, computadoras o celulares, que pueden ser obtenidos de forma voluntaria (entregados por victima o personas de interés) o de forma provocada (incautados como evidencias mediante diligencias de investigación, tales como registros con prevención de allanamiento o al momento de la captura del imputado) la información o las conversaciones que se han llevado a cabo entre víctima y acusado se pueden obtener mediante una pericia de "**EXTRACCION, ANALISIS, RESGUARDO DE INFORMACION ELECTRONICA, Y FIJACION DE IMÁGENES)** la cual puede ser practicada en fase administrativa (investigación fiscal) o en durante el proceso (casos judicializados bajo la jurisdicción y control de un juez o tribunal), sin embargo, en

ambos casos debe solicitarse como acto urgente de comprobación con la respectiva autorización judicial, y debe ser practicada por un perito permanente o accidental bajo las reglas del código procesal penal.

El hecho de que el contenido no quede almacenado en el servidor del administrador impide que la autoridad judicial pueda solicitar a la empresa prestadora del servicio que certifique el contenido de mensajes enviados o recibidos, teniendo que acudirse a los dispositivos electrónicos usados para su conversación.

Cuestión diferente será la de los datos de tráfico generados durante la conservación de WhatsApp y que no constituyen contenido de la conversación (origen y destino, ruta, hora, tamaño y duración de la comunicación).

Es preciso aclarar que las capturas de pantalla de las conversaciones en cualquier red social no constituyen prueba digital, solo meros indicios; al respecto la RAE define que hacer una captura de pantalla consiste en realizar una fotografía del contenido que se visualiza en un determinado momento en la pantalla de un dispositivo electrónico (*smartphone*, computadora, etc.) a través del propio dispositivo.

No obstante, lo anterior, la fijación de imágenes a través de capturas de pantalla que se realizan en una **EXTRACCION, RESGUARDO DE INFORMACION ELECTRONICA, Y FIJACION DE IMÁGENES, si constituye evidencia digital,** entonces, en el sentido descrito anteriormente, las capturas de pantalla podrían categorizarse como documentos electrónicos

4.5 La pericia informática

Según la legislación salvadoreña, la pericia informática o peritaje informático se enmarca principalmente dentro de la Ley Especial contra los Delitos Informáticos y Conexos, dado que, para la investigación y el juzgamiento de estos delitos, la prueba pericial informática es fundamental.

Los peritos informáticos son llamados a analizar la evidencia digital, los sistemas informáticos y los dispositivos electrónicos para determinar hechos relevantes para el caso.

Rol del Perito Informático (Perito en Informática):

El perito informático es un experto en tecnologías de la información y la comunicación que posee conocimientos especializados en áreas como el análisis forense digital, la seguridad informática, la recuperación de datos, el análisis de malware, entre otros.

Su función principal es proporcionar al juez o tribunal conocimientos técnicos especializados que no son de dominio común, para ayudar a esclarecer los hechos relacionados con un delito informático.

El perito puede ser designado por el juez a solicitud de las partes (Fiscalía, defensa) o de oficio, es decir puede ser un perito permanente o accidental.

Proceso del Peritaje Informático:

El proceso generalmente incluye la recolección, preservación y análisis de la evidencia digital, siguiendo protocolos forenses para garantizar su integridad y autenticidad.

El perito debe elaborar un informe pericial detallado que contenga la descripción de los procedimientos realizados, los hallazgos, las conclusiones y las recomendaciones, si las hubiere.

El perito puede ser llamado a testificar en juicio oral para explicar su informe y responder a las preguntas de las partes.

Principios específicos aplicables a las Pericias que involucran evidencia o prueba digital:

a) La objetividad, que implica que toda la evidencia, los rastros, las condiciones de los soportes evaluados, deben relacionarse y señalarse con precisión los parámetros técnicos utilizados para el análisis y la construcción de sus conclusiones.

b) La autenticidad y conservación. Que representa la obligatoriedad del especialista en conservar la integridad del contenido de la evidencia, su mismidad, para generar confiabilidad.

c) Legalidad. Verificar que la forma de obtener la fuente de prueba, sea respetando los presupuestos normativos, especialmente la no afectación o vulneración de derechos fundamentales.

Idoneidad. Implica que los medios probatorios y los procedimientos deben ser los pertinentes y suficientes para acreditar el thema probandum, lo que dependerá del tipo de evidencia digital, por ejemplo: respecto del contenido de un correo electrónico debe acreditarse el flujo, es decir, la información que permite identificar quiénes son los emisores y receptores del mensaje, pues generalmente uno de ellos está oculto, cómo se identifican las máquinas utilizadas y servidores, para lo que puede ser útil los geolocalizadores de los servidores. Además, el contenido del mensaje, para corroborar que se obtuvo el mensaje original libre de manipulaciones, que permitirá colegir la coherencia de su contenido; y finalmente, los

documentos o ficheros adjuntos, virus enviados, destinatarios ocultos o redireccionamientos intencionados

Validez de la Prueba Pericial Informática:

La prueba pericial informática es valorada por el juez según las reglas de la sana crítica, tomando en cuenta la idoneidad del perito, la claridad y fundamentación de su informe, y su testimonio en juicio.

En resumen, la pericia informática es una herramienta fundamental en el sistema de justicia salvadoreño para investigar y juzgar los delitos informáticos. Los peritos informáticos, como expertos en la materia, aportan conocimientos técnicos esenciales para el esclarecimiento de los hechos y la correcta aplicación de la ley.

Es importante tener en cuenta que esta información es una descripción general basada en las fuentes encontradas. Para obtener una comprensión completa y precisa de la legislación salvadoreña en materia de pericia informática, se recomienda consultar directamente los textos legales y buscar asesoramiento legal especializado.

4.7 La Prueba Digital en el Delito de Estafa Informática en El Salvador

La creciente digitalización de la sociedad salvadoreña ha traído consigo nuevas formas de criminalidad, siendo la estafa informática una de las más preocupantes. Este delito, que se aprovecha de la vulnerabilidad de los sistemas y la confianza de los usuarios en el entorno digital, requiere de herramientas probatorias específicas para su persecución y sanción. En este contexto, la prueba digital emerge como un elemento fundamental en la lucha contra la estafa informática en El Salvador.

La Ley Especial contra los Delitos Informáticos y Conexos de El Salvador, en su artículo 10, tipifica la estafa informática como la manipulación o influencia en el ingreso, procesamiento o resultado de datos de un sistema informático, con el objetivo de obtener un beneficio patrimonial indebido. Dada la naturaleza intrínsecamente digital de este delito, la prueba tradicional en formato físico a menudo resulta insuficiente o inexistente. Es aquí donde la prueba digital adquiere una relevancia crucial.

La prueba digital en casos de estafa informática puede manifestarse de diversas formas: Correos electrónicos fraudulentos, registros de transacciones en línea, direcciones IP, mensajes de texto, publicaciones en redes sociales, historiales de navegación, archivos informáticos, metadatos y cualquier otra información almacenada o transmitida electrónicamente pueden constituir evidencia valiosa para demostrar la comisión del delito, la identidad del autor y el perjuicio causado a la víctima.

Sin embargo, la obtención, preservación y presentación de la prueba digital en un proceso penal presentan desafíos particulares. La volatilidad de la información digital, su facilidad de alteración y la necesidad de garantizar su autenticidad e integridad son aspectos críticos que deben abordarse con rigurosidad. Es fundamental seguir una cadena de custodia clara y documentada desde el momento de la recolección hasta su presentación en juicio, asegurando que la prueba no ha sido manipulada.

En El Salvador, la legislación ha comenzado a reconocer la importancia de la prueba digital. Reformas al Código Penal han buscado incorporar como evidencia digital la información almacenada en medios tecnológicos, lo que facilita la persecución de delitos como la estafa informática, bajo esta categoría, los documentos digitales, mensajes electrónicos,

imágenes, videos, datos y cualquier tipo de información que sea almacenada, recibida o transmitida a través de las tecnologías de la información y comunicación o por medio de cualquier dispositivo electrónico, son admisibles como prueba y valorados.

Asimismo, el inciso segundo del artículo 259-A del código procesal penal, le reconoce valor de evidencia digital a la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, y su producción podrá ser realizada en el proceso penal mediante el uso de cualquier método y recurso tecnológico, que sea idóneo para realizar la correcta presentación de la misma, inclusive con el apoyo de perito informático que sean designado conforme a las reglas procesales establecidas en el CCP.

Lo anterior es importante, en razón que la prueba pericial informática es trascendental en el análisis y la interpretación de la prueba digital. Los peritos informáticos, con sus conocimientos especializados, pueden examinar los dispositivos electrónicos, analizar los datos, rastrear las comunicaciones y elaborar informes técnicos que ayuden al juez a comprender la evidencia digital y a tomar una decisión informada.

No obstante, debe tomarse en cuenta que la evidencia digital para que sea admitida en un proceso penal relacionado al delito de Estafa Informática debe cumplir los requisitos procesales relacionados a la obtención, resguardo o almacenamiento, y para que sea incorporada, producida y valorada, el ofertante deberá acreditar su autenticidad, lo cual puede ser realizado mediante el testimonio de la persona que intervino directamente en la elaboración,

generación, transmisión o recepción de la evidencia digital por medio de las tecnologías de la información y comunicación; acreditar que los mecanismos técnicos informáticos utilizados para su generación son los idóneos para asegurar esa autenticidad; y acreditar que el perito informático que haya intervenido en la obtención, resguardo o almacenamiento de la información o en el análisis de la evidencia digital, cuente con el conocimiento, experiencia, recursos tecnológicos apropiados para llevar acabo la pericia encomendado, sin importar si es un perito permanente o accidental, siempre y cuando su designación haya sido conforme a las reglas establecidas al respecto en el Código Procesal Penal.

Sin embargo, el cumplimiento de la anterior regla en el proceso de acreditación de autenticidad de la evidencia digital no garantiza una admisión y valoración automática, debido a que la parte contraria puede, de manera fundada, impugnar el mecanismo de acreditación dentro de la fase de instrucción formal, por lo que la parte interesada en la admisión de evidencia deberá demostrar su integridad por medio de la intervención de un perito informático

4.6 Agente encubierto digital como técnicas de investigación informática especializada

La Estafa Informática es un delito que se comete a través de medios informáticos mediante el abuso de las Tecnologías de la Información y la Comunicación, los rastros de su cometimiento se encuentran en información electrónica, conocida como evidencia digital, en ese sentido, la legislación salvadoreña, permite, como una técnica de investigación informática especializada, ordenar la realización de operaciones encubiertas digitales a cargo de un agente encubierto digital.

El agente encubierto digital, previa autorización judicial, será creado y administrado por personal técnico idóneo de la Policía Nacional Civil, con conocimiento y experiencia en la

materia, bajo el control directo del Fiscal a cargo de la investigación, quien hará constar la denominación y características del perfil utilizado por el agente encubierto; plataformas digitales donde se actuará; claves de acceso validadas y actividad concreta a desarrollar por el agente. Una vez concluida la intervención del agente encubierto digital, el Fiscal deberá dejar constancias de su existencia y actuación en el expediente fiscal.

Lo que se busca con esta técnica de investigación es que el agente encubierto digital, con autorización específica para ello, intercambié o envié por sí mismo cualquier tipo de información y archivos, interactúe y se relacione digitalmente a través de tecnologías de la información y de la comunicación con el objeto de: identificar o detener a los autores, partícipes o encubridores de un delito; impedir la consumación de un delito; o para reunir información o elementos de prueba necesarios para la investigación.

Por tratarse de operaciones encubiertas practicadas por la Policía, está permitido el uso de medios engañosos con el exclusivo objeto de investigar y probar conductas delincuenciales de carácter informáticos, previa autorización judicial, por lo que debe garantizarse que el agente encubierto digital esté exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de ésta y no constituyan una provocación al delito.

Si bien es cierto, la figura del Agente Encubierto Digital, se encuentra regulada en el artículo 259-D del código procesal penal, este no desarrolla el procedimiento para su implementación, por lo cual, como buena práctica y como un insumo orientativo, se propone, por el nivel de intromisión en la intimidad de los datos confidenciales, su nombramiento y autorización sea con autorización judicial, y la solicitud debe contener por lo mínimo:

Una relación fáctica de los hechos, a efecto de orientar y justificar la medida, con la descripción precisa del modus operandi, es decir, una descripción del cuando, como, donde, por qué y la técnica utilizada por el perpetrador para cometer el delito, ya que, lo que se pretende es tener una claridad de la escena del crimen.

Una descripción del fin concreto que se pretende con la implementación de la medida.

La individualización de los dispositivos o sistemas informáticos que serán objeto del registro, es decir, los medios utilizados para cometer el delito, contactos e interacción con la víctima.

La identificación de los mecanismos, metodología y herramientas mediante los cuales se almacenará la información obtenida que permitan asegurar la integridad de los datos y el resguardo de la cadena de custodia.

Descripción y acreditación de la persona designada para ejercer dicha función, a efecto de poder determinar, conocimiento y experiencia en la materia que lo conviertan en el personal idóneo para desempeñar dicho cargo.

La identificación de los perfiles o identidades digitales que utilizará el Agente Encubierto Digital, el cual en ningún caso podrá ser imágenes de personas reales.

- Establecer plazos específicos, los cuales podrán ser ampliados o reducidos, siempre y cuando el objetivo de la técnica así lo amerite

La cadena de custodia en la evidencia digital

La cadena de custodia digital no dista del concepto general de cadena de custodia desarrollado en el artículo 250 Pr.Pn, pues está referido proceso mediante el cual se garantiza que las personas que han intervenido durante su recolección, almacenaje o resguardo, analizar

y producción cuidaron de su inalterabilidad, el cual se documenta y permite garantizar la autenticidad de la evidencia y, en consecuencia, su confiabilidad que se haya protegido de: variaciones accidentales, intencionadas o acceso no acreditado, salvaguardando su validez y valor como prueba, debido a su trazabilidad garantizada.

Por lo que será necesario que toda actuación quede debidamente documentada por las personas vinculadas a las etapas procedimentales, que muestren las condiciones en las que han pasado de un estadio a otro, que evidencie la integridad y la autenticidad de la información contenida en la evidencia digital, por lo que en los registros deben constar las descripciones claras y precisas de: tipo de evidencia, forma de obtención, fechas de intervención, manera de resguardo y preservación, personas responsables de cada procedimiento, tipo de diligencias practicadas y las condiciones finales luego de la intervención controlada.

Para las evidencias digitales y su preservación concurren diferentes equipos y software especializados diseñados para facilitar la gestión de la cadena de custodia digital o electrónica, y para ello se ha creado normas y guías de buenas prácticas como RFC (Request for Comments), e ISO (International Organization for Standardization) y la norma ISO/IEC 27037 (Guía para la identificación, recolección, adquisición y preservación de evidencias digitales, 2012), entre otras, que permiten generar registros automáticos de las actividades desarrolladas, plataformas de almacenamiento con accesos controlados, entre otras virtualidades, las cuales son necesarias considerando que durante la investigación delictiva se tendrá acceso a

volúmenes altos de datos e información, formatos diversos, dispositivos diferentes que requerirán cuidados particulares por cada evidencia analizada[94].

En conclusión, la prueba digital es un elemento indispensable en la investigación y el juzgamiento del delito de estafa informática en El Salvador. Su correcta obtención, preservación y presentación, junto con un marco legal adecuado y la labor de los peritos informáticos, son fundamentales para combatir eficazmente esta forma de criminalidad y proteger a los ciudadanos en el entorno digital. A medida que la tecnología continúa avanzando, es crucial que el sistema legal salvadoreño siga adaptándose para garantizar que la justicia pueda alcanzar a quienes cometen delitos en el ciberespacio.

[94] "ISO/IEC 27037:2012:tecnología de la información, acceso 15 de mayo de 2025" https://www-iso-rg.translate.goog/standard/44381.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

5. CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

1. Las plataformas de comercio electrónico **simplifican** la compra y venta de bienes, servicios o productos mediante la internet, al mismo tiempo **aumentan** la perdida de privacidad, **reducen** costos y tiempo, pero **elevan** el riesgo de fraudes electrónico, por lo que, el riesgo debe gestionar en doble vía, por un lado, el cliente debe informarse antes de introducirse datos personales y financieros en páginas de comercio electrónico, y por su parte las empresas deben implementar las medidas de ciberseguridad que les permita evaluar y gestionar continuamente los riesgos de ciberseguridad que les permita el resguardo, el tratamiento de los datos personales y que garanticen el cumplimiento de las características mínimas de seguridad de la información, tales como integridad, disponibilidad y confidencialidad.

2. En estos últimos años, y debido a los efectos de la pandemia de COVID 19, nuevas modalidades de consumo y pago aceleraron la transición hacia una economía digital o en línea, puesto que en diversos país se estableció una restricción o hasta prohibición que las personas salieran de sus casas; estas nuevas modalidades fueron explotadas por los delincuentes para poder obtener ganancias ilícitas las cuales a su vez legitimaron aprovechando la disminución en las medidas de identificación o realización de operaciones presenciales.

3. En ese contexto progresaron los fraudes financieros, especialmente en la modalidad electrónica o en línea, donde los delincuentes aprovecharon la falta de conocimiento de los nuevos usuarios que, por el confinamiento comenzaron a realizar compras por internet y a usar medios de pago electrónicos, siendo las principales modalidad de fraude y delitos cibernéticos: **El Phishing**, el cual consiste en el envió de correos electrónicos fraudulentos, haciéndose pasar por una entidad, persona o empresa diferente, con el fin de extraer información de los clientes, generalmente contraseñas y credenciales de uso, que después son utilizadas para sustraer fondos de cuentas; **el Vishing**, consiste en llamadas telefónicas fraudulentas a personas de las cuales ya se tiene alguna información. El delincuente se identifica como una persona de alguna institución financiera o compañía con la que la víctima adquirió algún producto o servicio, generalmente indicando alguna falla o alerta en dicha adquisición, y tiene por objetivo obtener credenciales de acceso como contraseñas o números de token digital; y el **Smishing,** consiste en el uso de mensajes a celular por via de SMS o algún sistema de mensajería (WhatsApp, Telegram, Viber, Messenger, etc.) donde el emisor se hace pasar por una entidad financiera o compañía con la que la víctima tiene algún trato relación comercial, y se le informa de una anomalía u operación irregular, todo con el objetivo de obtener información financiera confidencial.

4. La nueva modalidad de consumo y pago en la economía digital generó una modificación en los perfiles de clientes que antes realizaban muy pocas o nulas operaciones vía internet, y que, ante las medidas de confinamiento decretadas en nuestro país, aumentaron sus consumos y gastos en línea lo cual levanto alerta en los sistemas automatizados, lo cual, en muchos casos, los delincuentes aprovecharon el cambio de patrones de comportamiento de

los clientes para ocultar operaciones ilícitas, como la rentabilidad de iniciativas de necios que operaban en línea.

5. Los fraudes financieros pusieron en evidencia otras vulnerabilidades que incrementan los espacios para que los delincuentes puedan obtener ganancias ilícitas, como lo son las capacidades limitadas en las entidades de orden público para hacer este tipo de investigaciones, relacionados a falta de herramientas tecnológicas, experiencia y recursos en las principales instituciones a cargo de investigar, procesar y condenar este tipo de flagelos como lo son: Fiscalía General del Republica, Policía Nacional Civil, y Corte Suprema de Justicia.

6. La clave para una investigación efectiva en delitos cibernéticos radica en el compromiso, cooperación y coordinación entre entidades del sector privado y público, es decir, las entidades privadas deben contar con políticas, procedimientos, controles, y herramientas que les permitan captar documentos, registros, que garanticen la integridad, oportunidad, confiabilidad y disponibilidad de la información allí contenida, para responder con prontitud a las solicitudes de información de la Fiscalía General de la República y de los tribunales competentes, en relación con el delito informático investigado. Tales registros servirán para reconstruir cada transacción, operación, o cambio, a fin de proporcionar, de ser necesario, pruebas de conducta delictiva por parte de los usuarios.

7. El Salvador ha realizado esfuerzos significativos para modernizar su marco legal en la lucha contra la delincuencia informática, principalmente a través de la Ley Especial contra

Delitos Informáticos y conexos promulgada en el año 2016 y que ha experimentado la fecha diferentes reformas encaminadas a incrementar en la penalidad de los delitos informáticos, asimismo se cuenta también con importantes reformas al Código Procesal penal encaminadas a introducir dentro del proceso Penal, la evidencia digital sumado a los refuerzos por volver más expedita la investigación y el proceso judicial de los delitos informativos.

8. El Salvador la figura de la gente digital encubierto es una herramienta crucial y relativamente reciente para la investigación de los delitos informáticos especialmente aquellos en los que delincuentes operan en el anonimato del ciber espacio; esta figura permitiría con su ejecución, la infiltración en redes o estructuras complejas de ciberdelincuentes, permitiendo la recolección de evidencia y se lograría individualizar al que esta al otro lado del servidor, navega en la darknet o se esconde tras una VPN.

9. El Salvador ha asumido el reto y el compromiso desde la esfera pública con las recientes creaciones de la ley de protección de datos y Ley de Ciberseguridad y Seguridad de la Información, de reconocer el valor de los datos almacenados y proteger los sistemas digitales y los datos personales del país, generando un marco de protección ante el actuar criminal que pueda beneficiarse de los mismos para el cometiendo de delitos informáticos.

5.2 RECOMENDACIONES

1. Por la naturaleza de los delitos informáticos todo el personal a cargo de la investigación, análisis, procesamiento, judicialización y condena, debe poseer capacidades, herramientas y conocimientos técnicos en la materia, por lo que se recomienda la creación de la Unidad Especializada en Ciberdelitos, tanto en la Fiscalía General de la República, como en las diferentes unidades de Investigación de la Policía Nacional Civil, así mismo, se recomienda la creación de tribunales especializados, es decir que solo tengan jurisdicción en delitos informáticos, jueces especializados en el manejo, tratamiento, valoración en materia de ciber delitos (adórnelo, este puede ser su aporte)

2. Desde el sector privado y público debe implementarse e intensificarse campañas radiales, televisivas y en redes sociales sobre los riesgos que conlleva introducir o proporcionar a terceros datos personales y crediticos, a efecto de evitar que se conviertan en víctimas de estafa informática o ser blanco de fishing.

3. Implementarse e intensificarse campañas radiales, televisivas y en redes sociales sobre los efectos penales en los que se puede incurrir por prestar cuentas bancarias, mulas financieras

4. Concientizar a las empresas para que fortalezcan sus sistemas de ciberseguridad para no ser víctima de este tipo de delitos.

5. La innovación debe buscarse siempre de manera responsable, debe prevalecer la cultura de cumplimiento, lo económico no debe de privar sobre la implementación de sistema de ciberseguridad para protección de datos.

6. Debe capacitarse a Fiscales y policías en la utilización y tecnificación de la implementación de la figura del agente digital encubierto como una técnica especializada de investigación.

7. Implementación de talleres prácticos con los diferentes sectores a cargo de la investigación, procesamiento y condena de este tipo de delitos, policías, fiscales jueces, sobre el manejo, utilización y valoración de prueba digital y tratamiento e implementación de agente digital encubierto.

8. A nivel de la FGR debe crearse e implementarse una guía para la implementación del agente digital encubierto como una técnica especializada de investigación, con el objeto de comenzar la implementación del mismo en los procesos judiciales vinculados a los delitos informáticos.

6. ANEXOS

GLOSARIO

BLOCKCHAIN: se entiende como una tecnología de registro distribuido (DLT) que permite almacenar información de forma inmutable, segura y descentralizada, sin necesidad de una autoridad central. Jurídicamente, se analiza en función de su capacidad para certificar transacciones con valor probatorio, gracias a su inmutabilidad y trazabilidad, Sustentar contratos inteligentes, que son acuerdos autoejecutables codificados en lenguaje informático o el garantizar la autenticidad y la integridad de los datos, lo que la convierte en una herramienta potencial para la prueba digital en procesos judiciales

CRIPTOMONEDA: es un activo digital que funciona como medio de intercambio, utilizando criptografía para garantizar la seguridad de las transacciones, controlar la creación de nuevas unidades y verificar la transferencia de activos. A diferencia del dinero tradicional, no existe físicamente y no está respaldada por un banco central.

CRIPTOACTIVOS: es un activo digital que utiliza criptografía y tecnologías como la blockchain (cadena de bloques) para garantizar su seguridad, trazabilidad y descentralización. Representa un valor o derecho que puede ser almacenado, transferido y negociado electrónicamente

DARKWEB (o web oscura): es una parte de internet que no está indexada por los motores de búsqueda convencionales (como Google o Bing) y que solo puede ser accedida mediante software especializado, como el navegador Tor. Se encuentra dentro de la Deep Web, pero representa su zona más oculta e intencionalmente anónima.

EXCHANGES: es una plataforma digital que permite a los usuarios comprar, vender o intercambiar activos financieros, como criptomonedas, divisas, acciones u otros instrumentos. En el contexto de las criptomonedas, un exchange funciona como una casa de cambio virtual, donde se pueden realizar transacciones entre diferentes monedas digitales o entre criptomonedas y dinero fiduciario.

FIDEICOMISO: es una figura jurídica mediante la cual una persona (llamada fideicomitente) transfiere bienes, derechos o recursos a otra (el fiduciario) para que los administre o disponga de

ellos conforme a un fin determinado, en beneficio de un tercero (el fideicomisario), según lo establecido en un contrato o testamento.

HACKER: es una persona con amplios conocimientos en informática y sistemas digitales, que utiliza sus habilidades para acceder, analizar o modificar sistemas informáticos, ya sea con fines legítimos o ilícitos. El término no implica necesariamente una conducta delictiva, aunque en el lenguaje común suele asociarse con actividades ilegales.

HTTP: es un protocolo de comunicación que permite la transmisión de información en la World Wide Web. Es el lenguaje que utilizan los navegadores y los servidores web para intercambiar datos, como páginas HTML, imágenes, videos y otros recursos.

INFORMATICA: es la ciencia que estudia el tratamiento automático de la información mediante el uso de sistemas computacionales. Su objetivo principal es almacenar, procesar y transmitir datos de forma eficiente, utilizando dispositivos electrónicos y programas especializados.

INTERNET: es la red mundial de computadoras interconectadas que permite el intercambio de información y comunicación entre usuarios de todo el planeta. Funciona mediante un conjunto de protocolos estandarizados, principalmente el TCP/IP, que permiten que los datos viajen de un punto a otro sin importar la distancia o el tipo de dispositivo.

IP: son las siglas de *Internet Protocol* o Protocolo de Internet, y se refiere al conjunto de reglas que rigen cómo se envían y reciben datos a través de una red. Su función principal es identificar de forma única a cada dispositivo conectado a una red, permitiendo que la información llegue correctamente a su destino.

SEGURIDAD DIGITAL: es el conjunto de medidas, prácticas y tecnologías destinadas a proteger la información, los sistemas y los dispositivos conectados a internet frente a accesos no autorizados, ataques cibernéticos, pérdida de datos o cualquier tipo de amenaza digital. Esta protege, Datos personales y sensibles (como contraseñas, información financiera o médica), Infraestructura tecnológica (servidores, redes, dispositivos), Identidad digital de personas y organizaciones, Disponibilidad e integridad de la información

SERVIDOR: es un sistema informático (hardware o software) que proporciona servicios, recursos o datos a otros dispositivos llamados clientes, a través de una red. Funciona bajo el modelo

cliente-servidor, en el cual el servidor responde a las solicitudes que hacen los clientes, como mostrar una página web, enviar un correo o almacenar archivos.

SOFTWARE: es el conjunto de programas, instrucciones y datos que permiten a una computadora o dispositivo electrónico realizar tareas específicas.

TRADING: es la actividad de comprar y vender activos financieros (como acciones, divisas, criptomonedas, materias primas, etc.) en los mercados con el objetivo de obtener beneficios a corto o mediano plazo.

WALLET: es una herramienta digital que permite almacenar, enviar y recibir activos digitales, como criptomonedas o tarjetas digitales. Aunque existen distintos tipos, todas cumplen la función de gestionar claves criptográficas que otorgan acceso a dichos activos.

7. Bibliografía

- Libros y Artículos

  - Aldana de Lara, Miriam Gerardine, Sandra Luz Chicas, Glenda Yamileth Baires, Samuel Aliven Lizama, Carlos Javier Rosa Monterrosa, y José Miguel Alas Alfaro. «Guia sobre evidencia digital en la legislación salvadoreña/ segunda edición.» San Salvador, s.f.

  - Alegsa, Leandro. *Definición de Keylogger (registrador de pulsaciones de teclas).* 12 de Junio de 2023. https://www.alegsa.com.ar/Dic/keylogger.php#gsc.tab=0 (último acceso: Febrero de 2025).

  - Asociación de Especialistas Certificados en Antilavado de Dinero, ACAMS. *Guía de estudio Certificado de Especialista en prevención de blanqueo de capitales.* 2024.

  - BASIC. *¿Quién es David Chaum?* s.f. https://academy.bit2me.com/quien-es-david-chaum/ (último acceso: Febrero de 2025).

  - Böhme, Rainer , Nicolas Christin, Benjamin Edelman, y Tyler Moore. *Bitcoin: Economics, technology, and governance.* Journal of Economic Perspectives, 2015.

  - Bravo, ESET - Christian Ali. *Spearphishing: Correos con asunto 'Nuevo Voicemail' intentan robar credenciales corporativas.* 06 de Febrero de 2025. https://www.welivesecurity.com/es/phishing/spearphishing-nuevo-voicemail-robo-credenciales-outlook/ (último acceso: Febrero de 2025).

  - Canto, Enrique Rovira del. *Delincuencia informatica y fraudes informáticos.* Granada: Comares, 2002.

  - CASANOVA, CARLOS ROMEO. *Enciclopedia Penal Básica.* Granada: Comares, 2002.

  - Catalini, Christian , y Joshua Gans. *Some Simple Economics of the Blockchain.* MIT Sloan Research Paper, 2016.

  - *Conceptos Básicos sobre Internet.* 2017. https://www3.uji.es/~pacheco/INTERN~1.html.

  - DEU, TERESA ARMENTA. «Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la

insuficiencia y la incertidumbre de 2018.» *Internet derecho y politia, IDPM dosier implicaciones juridicas* , 2018.

- Europol. *Internet Organised Crime Threat Assessment (IOCTA).* 2017.
- Financiera, Unidad de Investigación. En *Guía práctica para la investigación de criptoactivos: conceptos y estrategias avanzadas*. 2024.
- Financiera, Unidad de Investigación. «Estudio Estrategico Proveedores de Servicios de Activos Virtuales (PSAV).» Antiguo Cuscatlán, 2023.
- Fornell, Juan. *Bit2me Academy.* 6 de Marzo de 2023. https://academy.bit2me.com/que-es-una-red-p2p/.
- —. *Bit2Me Academy.* 15 de Febrero de 2023. https://academy.bit2me.com/wallet-monederos-criptomonedas/.
- Forouzan, Behrouz A. *Data Communications and Networking, 5a edición.* Mc Graw-Hill Education, 2013.
- Forouzan, Behrouz. *Comunicación de datos y redes de computadoras.* McGraw-Hill Education, 2017.
- Forrell, Juan. *¿Qué es un exchange de criptomonedas?* Octubre de 2019. https://academy.bit2me.com/que-es-exchange-criptomonedas/.
- —. *Bit2me Academy.* 15 de Febrero de 2023. https://academy.bit2me.com/wallet-monederos-criptomonedas/.
- Foundation, The Shadowserver. *The Shadowserver Foundation.* s.f. https://www.shadowserver.org/topics/botnets/ (último acceso: Febrero de 2025).
- GONZÁLEZ, EDMUNDO ARIEL DEVIA. «ESTAFA INFORMÁTICA DEL ARTÍCULO 248.2 DEL CÓDIGO PENAL.» Tesis, UNIVERSIDAD DE SEVILLA, Sevilla, España, 2017, 468.
- Google. *Actívate.* 2016. <http://google.es/activate> (último acceso: Febrero de 2025).
- Grupo de Acción Financiera de Latinoamérica GAFILAT. «Cuarta Actualización del Informe de Amenazas Regionales en materia de Lavado de Activos y Financiamiento del Terrorismo.» 2024.
- *La web del programador.* 2022. https://www.lawebdelprogramador.com/.

- LLOBREGAT, JOSÉ GARBERÍ. *Constitución y Derecho Procesal. Los fundamentos constitucionales del Derecho Procesal.* Madrid: Civitas-Thomson Reuters, 2009.
- LLUCH, XAVIER ABEL. *Derecho probatorio.* España: J.M. Bosch Editor, 2012.
- López, Jessica , y Mónica Sáenz Figueroa. *LA OBTENCIÓN DE LA PRUEBA PENAL INTERNACIONAL EN MATERIA DE DELITOS CIBERNÉTICOS.* Colombia, 2018.
- MARCOS, DAVARA FERNÁNDEZ DE. 2015.
- Ministerio de Seguridad de la Nación (Argentina). Protocolo General de Actuación destinado a primeros intervinientes para la identificación y secuestro de potenciales elementos de prueba de criptoactivos. Resolución 117/2025. Buenos Aires, 29 de enero de 2025.
- MORENO, MIRIAN HERRERA. «Revista de Actualidad Penal, número 39.» *El fraude informático en el derecho penal español.* Sevilla, 2001.
- National Democratic Institute. Manual de Ciberseguridad para Organizaciones de la Sociedad Civil: Una guía para las organizaciones de la sociedad civil que deseen iniciar un plan de ciberseguridad. Washington, DC: National Democratic Institute, 2022.
- Polaino, Miguel Navarrete. *Lecciones de Derecho Pena Parte General, tomo II segunda edición corregida y actualizada.* Editorial Tecnos, 2016.
- POLAINO, MIGUEL NAVARRETE. *Lecciones de Derecho Pena Parte General, tomo II, segunda edición corregida y actualizada.* Tecnos, 2016.
- Real Academia Española. *Diccionario de la lengua española.* 2024. https://dle.rae.es/inform%C3%A1tico (último acceso: 03 de 2025).
- Rodríguez, Antonio Morillas. *Redes de computadores: Principios, tecnologías y protocolos.* RA-MA, 2007.
- Rodríguez, Felipe. Derecho informático. El derecho en la era digital. La sociedad de información y el sistema jurídico. Contratos informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela jurídica del sistema informático. Córdoba: Universitas, 2013. Disponible en: http://www.feliperodriguez.com.ar/wp-content/uploads/2013/11/LIBRO-7-DERECHO-INFORMATICO.pdf

- Salamanca, Mtro. Leo Bladimir Benavides. *La Prueba Electrónica. Breves acotaciones sobre el documento electrónico.* San Salvador, s.f.
- Sarrabayrouse, Juan Manuel. *Delincuencia Informática Patrimonial.* Ediar, 2023.
- Sebesta, Robert W. *Concepts of programming languages (12ª ed.).* Pearson, 2019.
- *SecuriHub.* Diciembre de 2021. https://securihub.com/que-es-un-hash-criptografia-para-principiantes/.
- Seminario sobre Violencia y Paz. Nuevas fronteras en el reclutamiento digital: estrategias de reclutamiento del crimen organizado en TikTok. Ciudad de México: El Colegio de México, 2025. Disponible en: https://violenciaypaz.colmex.mx/publicacion/nuevas-fronteras-en-el-reclutamiento-digital-estrategias-de-reclutamiento-del-crimen-organizado-en-tiktok
- Soper, M. *Guía de introducción a la informática (6ª ed.).* Cengage Learning, 2019.
- Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). Guías prácticas para un abordaje integral del fenómeno: ciberdelito. Vols. I–III. Lima: UNODC, 2022.
- UIF. *UIF.* s.f. https://www.uif.gob.sv/

- Legislación

- Asamblea Legislativa de El Salvador. Ley de Creación del Fideicomiso Bitcoin. Decreto Legislativo No. 137. San Salvador, 31 de agosto de 2021. Disponible en: https://goldservice.com.sv/wp-content/uploads/2021/08/ley-de-creacion-del-fideicomiso-bitcoin.pdf
- Europa, Consejo de. Convenio sobre la Ciberdelincuencia (Convenio de Budapest). 2001.
- Ley Bitcoin Asamblea Legislativa de El Salvador. Ley Bitcoin. Decreto No. 57. Diario Oficial Tomo No. 431. San Salvador, 9 de junio de 2021. Disponible en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2020-2029/2021/06/E75F3.PDF
- Ley de Emisión de Activos Digitales Asamblea Legislativa de El Salvador. Ley de Emisión de Activos Digitales. Decreto Legislativo No. 643. San Salvador, 11 de enero de 2023. Disponible en:

https://www.asamblea.gob.sv/sites/default/files/documents/decretos/BED5A3F8-8937-4547-A291-CE06802B0B23.pdf

- Ley Especial contra delitos Informáticos y Conexos. San Salvador, San Salvador: Centro de Documentación Judicial, 2016.
- Reglamento de la Ley Bitcoin Presidencia de la República de El Salvador. Reglamento de la Ley Bitcoin. Decreto Ejecutivo No. 27. Diario Oficial Tomo No. 432. San Salvador, 27 de agosto de 2021. Disponible en: https://www.iscpelsalvador.org/wp-content/uploads/Reglamento-Ley-Bitcoin.pdf
- Reglamento de Proveedores de Servicios de Activos Digitales Comisión Nacional de Activos Digitales. Reglamento de Proveedores de Servicios de Activos Digitales. San Salvador, 11 de agosto de 2023. Disponible en: https://www.transparencia.gob.sv/descarga_archivo.php?id=NTk3NTYz