UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

ESCUELA DE POSGRADO

TRABAJO DE POSGRADO

LAS MODALIDADES DEL DELITO DE ESTAFA POR MEDIOS INFORMÁTICOS COMO CONSECUENCIA DE LA EVOLUCIÓN DEL COMERCIO ELECTRÓNICO DESDE LA PANDEMIA DE COVID 19.

PARA OPTAR AL GRADO DE

MAESTRO (A) EN DERECHO PENAL ECONÓMICO.

PRESENTADO POR

LICENCIADA LORENA ELIZABETH NOVOA POLANCO

LICENCIADO MIGUEL ANGEL CARCAMO IRAHETA

DOCENTE ASESOR

MAESTRO JOSÉ ANTONIO GARCÍA LIZAMA.

NOVIEMBRE, 2025

SANTA ANA, EL SALVADOR, CENTROAMERICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES

ING. JUAN ROSA QUINTANILLA QUINTANILLA

RECTOR

DRA. EVELYN BEATRIZ FARFÁN MATA

VICERRECTORA ACADÉMICA

M.Sc. ROGER ARMANDO ARIAS ALVARADO

VICERRECTOR ADMINISTRATIVO

LICDO. PEDRO ROSALÍO ESCOBAR CASTANEDA

SECRETARIO GENERAL

LICDA. ANA RUTH AVELAR VALLADARES

DEFENSORA DE LOS DERECHOS UNIVERSITARIOS

LICDO. CARLOS AMILCAR SERRANO RIVERA

FISCAL GENERAL

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

AUTORIDADES

M.Ed. ROBERTO CARLOS SIGÜENZA CAMPOS

DECANO

DR. JOSÉ GUILLERMO GARCÍA ACOSTA

VICEDECANO

LICDO. JAIME ERNESTO SERMEÑO DE LA PEÑA

SECRETARIO

M.Ed. MIGUEL ANGEL CRUZ

DIRECTOR DE LA ESCUELA DE POSGRADO

Abreviaturas que se usarán dentro del presente capítulo:

N°	Abreviatura	Concepto
1	Art.	Articulo o Articulos
2	Cn.	Constitucion de la Republica de El Salvador
3	CP.	Codigo Penal Vigente
4	CPP	Codigo procesal Penal
5	LCAT	Ley Contra Actos de Terrorismo
6	LEDIC	Ley Especial de Delitos Informáticos y Conexos
7	RAE	Real Academia Española
8	TIC´s	Tecnologías de la Información y Comunicación

INDICE

INTRODUCCIÓN

El presente Proyecto de investigación ha sido elaborado por estudiantes de la Maestría en Derecho Penal Económico, para ser entregado a la Acción Académica: Seminario de Investigación I: Apuntes de Metodología de la Investigación, Ciclo II-2023.

El propósito de elaborar el presente proyecto, es para tener certeza de las nuevas formas de criminalidad económica mediante la comisión de estafas por medios electrónicos como consecuencia del aumento significativo del comercio a través de internet derivado de las limitaciones a la libertad de circulación impuestas a la población como consecuencia de la cuarentena domiciliar obligatoria impuesta por el Estado como una forma de controlar y combatir el contagio y la propagación masiva del covid-19 en la población.

El proyecto de investigación se desarrollará por etapas donde se van exponiendo de forma clara y detallada el planteamiento de la problemática, luego se harán consideraciones teóricas y doctrinarias al delito de estafa, modalidades comunes del delito de estafa, comercio informático a través de internet, redes sociales y otras plataformas electrónicas, asi mismo, se expondrán las nuevas modalidades de estafas electrónicas y sus diferencias con el incumplimiento de contrato.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Planteamiento del problema

El 11 de marzo de 2020, en la Ciudad de Ginebra Suiza, el Director General de la Organización Mundial de La Salud (OMS), el doctor Tedros Adhanom Ghebreyesus, anunció que la enfermedad por el coronavirus 19 (COVID-19) puede caracterizarse como una pandemia. "La OMS ha estado evaluando este brote durante todo el día y estamos profundamente preocupados tanto por los niveles alarmantes de propagación y gravedad, como por los niveles alarmantes de inacción. Por lo tanto, hemos evaluado que COVID-19 puede caracterizarse como una pandemia", afirmó. (Salud, 2020)

Por Decreto Ejecutivo (RAMO DE SALUD) No. 4 se decreta cuarentena de 30 días derivada de la declaratoria de Pandemia por COVID-19 a todas aquellas personas que ingresen al territorio salvadoreño por cualquier vía, publicado en el diario oficial del 11 de marzo del año 2020. (transparencia.gob.sv, 2020)

Por Decreto Legislativo número 593 de fecha catorce de marzo de dos mil veinte la Asamblea Legislativa de El Salvador estableció "ESTADO DE EMERGENCIA NACIONAL DE LA PANDEMIA POR COVID-19. Dicho cuerpo normativo, establece directrices para la contención de la pandemia.

Por Decreto Ejecutivo (RAMO DE SALUD) No. 7 publicado en el Diario Oficial del 16 de marzo del año dos mil veinte se adoptaron medidas de contención para actividad comercial y recreativa por la pandemia de COVID-19. (transparencia.gob.sv, 2020)

Por Decreto Ejecutivo (RAMO DE SALUD) No. 12 publicado en el Diario Oficial del 21 de marzo del año dos mil veinte, se adoptaron medidas Extraordinarias de Prevención y Contención para Declarar el Territorio Nacional como zona sujeta a Control Sanitario, a fin de contener la pandemia de COVID-19, vigencia de 30 días. Ninguna persona podía circular o reunirse en el territorio de la República, salvo las excepciones que contenía dicho decreto. (transparencia.gob.sv, 2020)

Las regulaciones citadas con anterioridad establecieron limitaciones a derechos fundamentales, especialmente al derecho a la libre circulación de los ciudadanos en el territorio nacional, permitiendo la circulación a personas que brindaban servicios esenciales a la población, como salud, alimentación, seguridad, entre otros; siendo que, la cuarentena domiciliar obligatoria no solo implicó una restricción a la libertad ambulatoria de la población, sino que también la paralización parcial de la economía nacional por el cierre de empresas y negocios.

El trabajo presencial fue sustituido por el teletrabajo, trabajo desde casa o trabajo en línea como una forma de desempeñar las actividades laborales de forma no presencial, total o parcialmente, por tiempo determinado o de manera indefinida, fuera del centro de trabajo y utilizando como soporte las tecnologías de la información y comunicación. Dicha modalidad de trabajo fue aprobada por la Asamblea Legislativa durante el mes de agosto de 2020, como una estrategia para prevenir los contagios de COVID- 19, mediante la prórroga de la Ley de Servicios Internacionales. (SALVADOR, ASAMBLEA.GOB.SV, 2022)

Todas las medidas para prevenir contagios y contener el COVID-19, surtieron efectos negativos en la economía, sin embargo, el ingenio del ser humano y la necesidad de abastecerse de servicios y bienes esenciales para la subsistencia contribuyeron al incremento del comercio electrónico a nivel nacional e internacional.

Según estudio realizado por Mercados & Finanzas, el comercio electrónico en El Salvador aumentó en un 83% en 2020. " Las restricciones de movilidad impuesta para reducir contagios a causa de la pandemia del Covid-19 hicieron emerger la creatividad de las personas y empresas. El comercio electrónico pasó a ser una actividad principal y, en muchos casos, la única manera que proveedores encontraron para hacer llegar sus productos a clientes y sobrellevar la crisis.

Esta modalidad de intercambio a través de redes sociales u otros medios electrónicos tuvo un incremento del 83% en El Salvador en 2020, así lo determinó una encuesta desarrollada por la Defensoría del Consumidor." (FINANZAS, 2021)

Con el aumento de la actividad económica a través de las tecnologías de la información también se incrementaron los índices de criminalidad informática en el país entre ellos hurtos

y estafas por medios informáticos; siendo que a evolución económica ha traído ventajas al desarrollo de la economía, pero también ha generado problemas y vulnerabilidad de los consumidores al no existir contacto directo entre fabricantes, vendedor/a y consumidores finales (KPMG, riesgos del e-commerce a raíz del covid-19, 2021). En ese sentido se da la vulnerabilidad de los consumidores/as, y se enlistaron nuevas formas de comisión de delitos entre ellos, la estafa, por medio o por la via electrónica, ya que, como resultado de la pandemia no era permitido en un primer momento el contacto directo entre personas por los altos riesgos de contagios a nivel nacional e internacional.

La fiscalía General de La República (FGR) registró en 2021 más de 6,000 casos de estafa y hurto por medios informáticos, según el balance de los delitos con mayor incidencia de ese año, divulgados por el fiscal general. Los datos revelan una alarmante tendencia al alza en varios delitos, especialmente los relacionados al hurto de identidad. (MUNDO, 2021)

1.2.1 Delimitación del problema.

Teórica.

Se retomará información de instituciones gubernamentales y no gubernamentales oficiales y confiables en sus análisis, doctrina y resultados investigativos para filtrarlos y hacer una base sólida en la cual se comenzará a investigar con datos, e información fidedigna. Es por ello, que inicialmente se ha retomado el marco jurídico legal del contexto en el que se dio mayor crecimiento, como se ha venido mencionando en párrafos anteriores, en contexto de pandemia y post pandemia, y se han incorporado los Decretos Ejecutivos y Legislativos que le dieron vida al resguardo obligatorio y a mayor comercio por internet como consecuencia de la primera, y así sucesivamente.

1.2.2 Espacial

El lugar de investigación será determinado en relación al territorio, ya que el problema planteado abarca modalidades de estafa a nivel nacional e internacional, sin embargo, será enfocado a nivel nacional, con énfasis en los casos judicializados; entonces, la problemática expuesta será analizada solo a nivel de la circunscripción territorial salvadoreña, tomando como parámetro el incremento de la actividad económica a través de las tecnologías de la comunicación a partir del año 2020 a la fecha, ya que si bien es cierto, ya no existen restricciones tan estrictas para la prevención del COVID-19, pero el comercio electrónico sigue en aumento, por ende la criminalidad electrónica también sigue en tendencia al alza.

CAUSA	AQP	CONSECUENCIAS
Internet y Redes Sociales	**A: ¿Adónde?** ● **Plataformas electrónicas** ● **Redes Sociales**	**Engaños en línea** **Desfalcos monetarios** **Delitos informáticos**
Contratos no formalizados y verbales	**Q: ¿Quiénes o qué?** ● **Compradores** ● **Vendedores**	**Relación abusiva y engañosa de uno o de ambas partes**
Ardid o engaño en el comercio	**P: ¿Qué Problemas tienen?** ● **Perfiles falsos** ● **Estafas**	**Consumación de ilícitos en contra del patrimonio, transacciones y otros.**

1.2.3 Temporal

Se abordará donde se desarrolla la situación o problema de investigación, y se fijará el tiempo o período de la vida del fenómeno que se investigará, siendo que en el devenir de la problemática han surgido mutaciones a comisiones delictivas más especializadas, con variantes en la recurrencia, modalidad, y tácticas para evadir a la justicia y dejar a las víctimas sin evidencias claras para una futura investigación judicial y que exista elementos de prueba suficientes para poner tras las rejas a los/las culpables.

1.3.1 Unidades de análisis

A) Institucionales (procesos conocidos por la defensoría del consumidor)

B) Operadores de Justicia en cuanto a condenas efectivas y reparación de daños

1.4.1 Objetivos de investigación

1.4.2 Objetivo general:

Identificar las nuevas modalidades de Estafas por medios electrónicos o redes sociales como consecuencia del aumento del comercio electrónico desde la pandemia de COVID-19.

1.4.3 Objetivo específico:

- Clasificar las modalidades de oferta, demanda, negociación y adquisición de bienes y servicios a través de medios informáticos en El Salvador.
- Determinar las Plataformas electrónicas más utilizadas para el comercio electrónico a nivel nacional.

- Indagar los medios más comunes de pago de los bienes y servicios adquiridos y la posibilidad de comisión de delitos fiscales, lavado de activos y hurto por medios informáticos en dicha modalidad de pago en El Salvador.

2.4 Cuestionario de investigación.

Preguntas generales:

- ¿Han mutado las modalidades para cometer el delito de estafa?
- ¿Cuándo estamos ante el incumplimiento de contrato y ante una estafa a través de redes sociales?
- ¿Cuál es el rol de los contratos criminalizados en el comercio electrónico?
- ¿La regulación penal actual, puede combatir las estafas electrónicas?
- ¿Que seguridad genera el sistema bancario nacional en las transacciones electrónicas?
- ¿ Qué tribunales son competentes para conocer casos de estafas electrónicas a nivel internacional?.

2.5 Justificación.

Es importante esta investigación porque primeramente debemos visualizar la problemática y su alarmante auge en los últimos tiempos post pandemia, y de la misma forma al describir, analizar y detectar cómo es este fenómeno delictivo, y su estructura y procesos, podremos hacer un diagnóstico para buscar posibles soluciones a la problemática, en un mundo globalizado, donde la economía y el internet al permeado todos los aspectos de la vida, incluyendo obviamente el ámbito del camino del delito, su tipicidad o atipicidad, o inclusiva la ampliación en cuanto a los criterios jurisprudenciales de tipicidad y legalidad para abordar este flagelo moderno, como lo es las Estafas Electrónicas y su diferencia con otros tipos delictivos que pueden llegar a confundir en cuanto a los tipos penales y sus características propias, consecuencias jurídicas a nivel particular (víctima, victimario) como también a nivel ampliado (social o nacional en el tracto judicial general)

Es por ello que se ha decidido estudiar este campo del derecho donde la actividad de las instituciones públicas es clave para su persecución y monitoreo respectivo, como garante de la legalidad, siendo algunas de las más destacada, la Defensoría del consumidor protegiendo a las y los ciudadanos, en sus relaciones de demanda y oferta y las normativas aplicables se cumplan en su mayor esplendor, salvaguardando la seguridad jurídica; además también la Fiscalía General de la República junto con el Órgano Judicial, salvaguardando el

principio de igualdad, legalidad , lesividad y Justicia, ante la comisión de un hecho delictivo, que se aplique el derecho y sus consecuencias jurídicas de las resultas del debido proceso.

2.6 Viabilidad de la investigación

Es viable porque es un tema de relevancia jurídica, ya que todos y todas podemos ser potenciales víctimas de delincuentes "cibernéticos" en nuestras operaciones o transacciones por internet, desde la compra de una hamburguesa hasta la compra de una casa, en donde el/la vendedor/ra y comprador/ra no es necesario que se conozcan, ni tampoco que tengan algún contacto físico para realizar y concretar una venta. En ese sentido es importante mencionar que las fuentes de información a consultar ya tenemos los primeros acercamientos y las estamos activando preliminarmente están accesibles para brindar información fidedigna sobre datos concretos sobre la temática, en relación al tiempo requerido tenemos, en cuanto al tiempo requerido seria dependiendo la información que se solicite y su complejidad, el análisis respectivo y el tiempo de respuesta de las instituciones, y en cuanto a las condiciones para realizar la investigación también son accesibles.

2.7 Límites y alcances

En cuanto a los límites se podría prever los tiempos de respuestas de las instituciones para entregarnos información solicitada, o bien que no sea autorizada a pesar de haber sido legalmente solicitada, algunas reservas de los casos más emblemáticos fenecidos, o la negativa a algún caso en particular.

En cuanto a los alcances con el análisis y las resultas de la investigación podremos hacer aportes y verter opiniones en la que se recomiende alguna acción en concreto o bien alguna crítica constructiva en donde se señale algún tipo de responsabilidad en algún mandato de ley o falencias en el área judicial.

CAPÍTULO II: MARCO DE REFERENCIA

2.1 Antecedentes del problema:

"NEGOTIA ET DELICTA".- La presencia del dinero en la conciencia del hombre actual estimula al máximo su energía y lo ha hecho evolucionar, pero en un sentido especulativo y pragmático, calculador e interesado.

EL COMERCIO COMO EXPRESIÓN DE NEGOCIO EN LOS PUEBLOS ANTIGUOS.- cuando la familia era de signo patriarcal, puede decirse que no existía el comercio. El patriarca totalizaba en sus manos y en su voluntad todos los poderes. Sin embargo, aparece una forma primaria de trueque, primero entre los individuos y después entre los grupos. El espíritu inventivo hace nacer al "artesano", que elaboraba objetos para sí y también para otros.

Con la aparición de la mercadería intermedia-*el dinero*- se inició una nueva faz económica, la monetaria, y su característica de los primeros tiempos fue el *nomadismo.*

A LA PAR DE LOS "NEGOTIA" SURGEN LOS "DELICTA".- el peregrinaje de los mercaderes habría de crear un fenómeno paralelo: el de los piratas. La piratería apareció en aquellos tiempos como la sombra del comercio, tanto en tierra como por mar. (VÁSQUEZ, 2004)

La globalización ha generado una expansión económica a nivel mundial, la economía actual se vale de herramientas tecnológicas como el internet para facilitar la intercomunicación entre seres humanos, sin necesidad de desplazarse de un lugar a otro, sin embargo, la mercadería, mantiene la característica de "*nomadismo*", desde el lugar donde se produce, hasta donde se recibe o se consume.

El fenómeno de la globalización fue impulsado desde los años sesenta cuando se desarrollaban las primeras computadoras en las principales universidades y centros de investigación del mundo, que solo estaban al alcance de las grandes universidades y de las oficinas gubernamentales de defensa. Los científicos y profesores, trabajaban en sus propios proyectos y deseaban compartir sus experiencias con sus colegas (que la mayoría de veces se encontraban en lugares diferentes)

El Internet se inició en torno al año 1969, cuando el Departamento de Defensa de los EE: UU desarrolló ARPANET, una red de ordenadores creada durante la guerra fría cuyo objetivo era eliminar la dependencia de un Ordenador Central, y así hacer mucho menos vulnerables las comunicaciones militares norteamericanas. Específicamente el día 7 de abril de 1969, se recuerda como el nacimiento del internet. Se trata de la publicación del RFC-1 (RequestForComments No. 1), documento que describe el protocolo empleado por los equipos utilizados para interconectar la primera red computacional, ARPANET(Red de la Agencia de Investigación de Proyectos Avanzados). En octubre del mismo año se envió un mensaje de un computador a otro: Charly Kline, un estudiante de la UCLA, tecleo un mensaje que decía "login", lo cual tenía que viajar unos 500 KM de distancia para que llegase al receptor. Fue en ese momento cuando el profesor Leonard Kleinrock de la Universidad de Stanford, recibió el mensaje, aunque solo llegaron las vocales "O" e "I". (GUADALAJARA)

Desde su surgimiento hasta la fecha, el internet ha tenido una gran evolución en materia tecnológica y expansión territorial, lo que usualmente se hacía en los años sesenta con ordenadores grandes y lentos hoy se puede hacer a través de un dispositivo que cabe en el bolsillo "el teléfono celular".

Desde la época del nomadismo a la época actual, en lo referente a la interacción y comercio de forma personal hay una gran brecha tecnológica que facilita la intercomunicación entre personas en cualquier lugar del mundo, mucho ha tenido que ver la competencia entre los desarrolladores de teléfonos inteligentes, quienes cada vez brindan mayores utilidades; así como también las grandes mentes de la informática que fueron capaces de convertir el internet en un mundo virtual de interacción personal a través de las redes sociales.

"Las redes sociales son lugares en internet donde las personas publican y comparten todo tipo de información, personal y profesional, con terceras personas, conocidos y absolutos desconocidos", afirma Celaya (2008). Por su parte, Wikipedia la define como: "una estructura social que se puede representar en una forma o varios grafos donde nodos representan individuos y las aristas la relaciones entre ellos"

Más allá de las definiciones puntuales, de lo que semánticamente representa una red

social, lo cierto del caso es que ha sido un espacio creado virtualmente para facilitar la interacción entre personas. Desde luego, esta interacción está marcada por algunos aspectos particulares como el anonimato total o parcial, si así el usuario lo deseara, la facilidad de contacto sincrónico o anacrónico, así como también la seguridad e inseguridad que dan las relaciones que se suscitan por esta vía. (Hutt Herrera, 2012).

La facilidad en la intercomunicación ha permitido el intercambio de mercancías entre usuarios de internet "NEGOTIA", utilizando la web como una especie de vitrina virtual para el ofrecimiento de productos y servicios, generando flujo de dinero entre los negociantes, lo que genera la aparición del "DELICTA" o delitos informáticos de índole patrimonial a través de la web.

Los orígenes de los delitos informáticos pueden rastrearse a partir de los años 60s por el temor infundido por la literatura de la época en relación a la recolección y almacenamiento de datos personales en computadoras. Este tiene como referencia la obra de "1984" de George Orwell, donde un Gran Hermano omnipresente controlaba y vigilaba a las personas a través del uso de las tecnologías. Tras la publicación de artículos periodísticos sobre algunos de los casos apareció por primera vez el término *delitos informáticos o delincuencia relacionada con computadoras,* retomado posteriormente por la literatura fantástica de la época para la publicación de obras relacionadas dentro de un género definido posteriormente como "cyberpunk" (SAIN)

En lo que respecta a El Salvador se ha reconocido la existencia de delitos informáticos a través de una ley denominada "LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS", emitida mediante decreto número 260 del cuatro de febrero del año dos mil dieciséis.

La referida ley reconoce la existencia de un problema de criminalidad informática en sus considerandos III y IV, los cuales literalmente dicen "… III. Que en la actualidad, los instrumentos electrónicos por medio de los cuales se envía, recibe o resguarda la información, han adquirido una especial relevancia, tanto a nivel internacional como nacional, para el desarrollo económico, político, social y cultural del país; por lo que se vuelve prioridad del Estado, proteger dicha información, ya que al no protegerla se atenta contra la

confidencialidad. Integridad, seguridad y disponibilidad de datos en general; y…" "…IV Que esta diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación, no se encuentra suficientemente reguladas en nuestra normativa penal vigente, generando una impunidad para quienes cometen estos tipos de delitos; en consecuencia, resulta necesaria su tipificación y la adopción de mecanismos suficientes para facilitar su detección, investigación y sanción de estos nuevos tipos de delitos…"

2.2 Teorías y conceptos básicos:

Teoría general de la estafa: "cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, reduciéndolo a realizar un acto de disposición en perjuicio propio o ajeno"

De esta definición se deducen los distintos elementos esenciales para la existencia de la estafa: engaño, error, disposición patrimonial y perjuicio. Entre engaño y perjuicio debe mediar una relación de causalidad de tal manera que el engaño sea el motivo o causa del perjuicio. Si falta esta relación no existe estafa. (MUÑOZ CONDE, 2004).

Los conceptos fundamentales que integran el delito de estafa son complementarios entre si y no pueden ser excluyentes, de tal manera que cuando se realizan en conjunto, se configura un delito de estafa; es necesario fraccionar cada uno de sus conceptos para una mejor comprensión y explicación: **a) Engaño:** por engaño debe entenderse cualquier acción u omisión del hechor, encaminada a ocultar la realidad, mediante simulación de una realidad distinta, o alteración de la realidad verdadera; **b) Error:** el error se materializa cuando el perjudicado por el delito acepta la realidad simulada o alterada del sujeto activo; **c) Disposición Patrimonial:** consiste en el uso de bienes tangibles de parte de la víctima a favor del delincuente o de un tercero; **d) Perjuicio:** debe entenderse por perjuicio la afectación que sufre la víctima del delito de estafa, afectación que no solo comprende la disposición patrimonial, sino también otras consecuencias que se generen del hecho delictivo, que determinarán la dosimetría de la pena a imponer.

Delito informático: de conformidad con el artículo 3, literal a) de la Ley Especial Contra Delitos Informáticos: " 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."

Redes sociales: según la citada ley Especial Contra Delitos Informáticos, en su artículo 3, literal q) es la estructura o comunidad virtual que hace uso de medios tecnológicos y de la comunicación para acceder, establecer y mantener algún tipo de vínculo o relación mediante el intercambio de información.

Estafa informática: el legislador ha configurado un tipo penal especial del delito de Estafa y lo ha definido con una serie de conductas sancionadas con pena de prisión en el artículo 10 de la Ley Especial Contra Delitos Informáticos el que literalmente dice: "… el que manipule o influya 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 o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para si o para otro, en perjuicio patrimonial ajeno, será sancionado con prisión de cinco a ocho años.

Los conceptos y teorías enunciadas con anterioridad son de vital importancia para identificar y diferenciar la estafa en su modalidad común y la estafa informática, ya que desde un punto de vista teórico y práctico comparten algunas similitudes, pero también existen diferencias entre ambos delitos.

2.3 Marco jurídico

Por decreto número 1030 del treinta de abril de mil novecientos noventa y siete, la Asamblea Legislativa de El Salvador aprobó el Código Penal contemplando en su título VIII los delitos relativos al patrimonio, y en el capítulo III las Defraudaciones.

En el catálogo de las defraudaciones se incluyen dos modalidades de estafa, la Estafa y la Estafa agravada.

Estafa Art. 215.-

EL QUE OBTUVIERE PARA SÍ O PARA OTRO UN PROVECHO INJUSTO EN PERJUICIO AJENO, MEDIANTE ARDID O CUALQUIER OTRO MEDIO DE ENGAÑAR O SORPRENDER LA BUENA FE, SERÁ SANCIONADO CON PRISIÓN DE DOS A CINCO AÑOS SI LA DEFRAUDACIÓN FUERE MAYOR DE DOSCIENTOS COLONES.

Para la fijación de la sanción el juez tomará en cuenta la cuantía del perjuicio, la habilidad o astucia con que el agente hubiere procedido y si el perjuicio hubiere recaído en persona que por su falta de cultura o preparación fuere fácilmente engañable.

Estafa agravada Art. 216.-

El delito de estafa será sancionado con prisión de cinco a ocho años, en los casos siguientes:

1) Si recayese sobre artículos de primera necesidad, viviendas o terrenos destinados a la construcción de viviendas;

2) Cuando se colocare a la víctima o su familia en grave situación económica, o se realizare con abuso de las condiciones personales de la víctima o aprovechándose el autor de su credibilidad empresarial o profesional;

3) Cuando se realizare mediante cheque, medios cambiarios o con abuso de firma en blanco;

4) Cuando se obrare con el propósito de lograr para sí o para otro el cobro indebido de un seguro;y,

5) Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos.

La Ley Especial Contra Delitos Informáticos también regula una modalidad de estafa denominada “Estafa informática” que comparte elementos con la estafa del artículo 215 del Código Penal y del artículo 216 numeral 5) del código relacionado.

Estafa informatica.

Art. 10.- 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, en perjuicio patrimonial ajeno, será sancionado con prisión de cinco a ocho años.

Se sancionará con prisión de ocho a diez años, 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.

En ambos casos estafa común y estafa electrónica, se requiere que la acción penal sea ejercitada previa instancia particular, de conformidad con el artículo 17 del Código Procesal Penal, siendo el agraviado por el delito, quien deba accionar el sistema de justicia por medio de la Fiscalía General de La República, teniendo la disposición de la acción penal durante el procedimiento.

ANÁLISIS COMPARATIVO ENTRE ESTAFA COMÚN Y ESTAFA ELECTRÓNICA

ELEMENTOS DEL TIPO PENAL	ESTAFA COMÚN DEL ARTÍCULO 215 DEL CÓDIGO PENAL	ESTAFA INFORMÁTICA DEL ARTÍCULO 10 DE LA LEY DE DELITOS INFORMÁTICOS
ELEMENTOS OBJETIVOS DEL TIPO PENAL	**Uso de ardid o cualquier medio engañoso para sorprender la buena fe de la víctima o de un tercero**	**Manipulación, influencia en el ingreso o procesamiento de un sistema tecnológico mediante el uso indebido de datos o programación o cualquier otra acción fraudulenta que incida en el procesamiento de datos o de como resultado información falsa.**
ELEMENTOS NORMATIVOS DEL TIPO PENAL	**Provecho injusto en perjuicio ajeno si la defraudación es superior a doscientos colones o su equivalente en dólares**	**Beneficio patrimonial indebido para sí o para otro, en perjuicio patrimonial ajeno. Sin establecer cuantía mínima**
ELEMENTOS SUBJETIVOS DE LOS TIPOS PENALES	**El tipo penal es eminentemente doloso, requiere conocimiento de la ilegalidad que se está cometiendo y la voluntad**	**Se trata de un delito doloso, donde el hechor no solo tiene conocimiento de la ilicitud de su actuar, sino un conocimiento**

	de ejecutarla	**informático necesario para la ejecución del delito.**
CONSECUENCIA JURÍDICA	**Pena de prisión de dos a cinco años en el tipo básico y de cinco a ocho años en su modalidad agravada**	**Pena de prisión de cinco a ocho años en el tipo penal simple y de ocho a diez años en modalidad agravada.**

Contextualización:

Con el aumento de las tecnologías de la comunicación y de la información ha ido disminuyendo la brecha digital entre los seres humanos, facilitando el comercio electrónico entre desconocidos que posiblemente nunca lleguen a conocerse, modificando sustancialmente la oferta y la demanda como la conocemos.

Esa interacción detrás de un ordenador, detrás de un teléfono inteligente o cualquier otro dispositivo que permita la conexión a internet, también puede ser utilizada para ofertar productos y servicios inexistentes, bien sea que los mismos existan pero que una vez obtenido un beneficio no sean proporcionados al cliente, hasta casos excepcionales donde personas detrás de perfiles falsos establecen relaciones sentimentales y obtienen dinero por medio de engaños a sus víctimas.

Es interesante que, en el delito de estafa electrónica, el legislador no establece cuantía, por lo que no existe un criterio objetivo para determinar cuándo es procedente ejercer la acción penal por dicho delito, quedando a criterio de la autoridad fiscal determinar si procede accionar o no, el sistema de justicia.

Al tratarse de un comercio electrónico masivo, la exposición a caer en una estafa electrónica aumenta en proporción al delito de estafa común y al no existir una cuantía que determine el monto de la afectación patrimonial, pudiésemos estar hablando de estafas masivas con afectación a nivel nacional. Por lo tanto, la presente investigación se realizará a nivel nacional, tomando como punto central las principales plataformas que facilitan el

comercio electrónico.

2.4 Estado del arte:

En relación a este tema, se indago sobre la base de otros autores o profesionales que hablan sobre el tópico en comento, cuales son sus conclusiones y su visión sobre la Estafa Informática en El Salvador, es por ello, que tenemos la investigación científica de los licenciados José Heriberto Carranza y Daisy Arely Hernandez, quienes abordaron recientemente la temática de la Estafa Electrónica en el Salvador (Universidad de El Salvador, año 2022) y su enfoque principal es una investigación descriptiva en donde sentaron las bases para conocer cómo está el conocimiento o información de la población Salvadoreña y los operadores de justicia en general, a la vez que se realizó una comparación a grandes rasgos del delito de la Estafa informática con otras legislaciones internacionales, en ese orden de ideas, al desarrollar la etapa descriptiva y analizar los resultados de como esta la socialización de este delito, se concluye con las siguiente información:

1- "El internet fue creado principalmente como un medio entre las personas, utilizándose para hacer transacciones bancarias y para el comercio electrónico a través de aplicaciones que resultaron útiles; posteriormente este comercio se ha visto afectado por el surgimiento de la delincuencia digital donde se ha utilizado la tecnología y la comunicación para cometer estafas electrónicas logrando obtener un beneficio patrimonial indebido de las personas que resultan afectadas." (Carranza, J.; Hernández, D. Universidad de El Salvador,2022).
2- "El surgimiento del delito de estafa se dio en el Código Penal de 1826 de manera tradicional y en el código Penal de 1998 se incorporaron agravantes a este delito entre ellas, la manipulación que interfiera el resultado de un procedimiento o transmisión informática de datos, pero en vista de los avances tecnológicos y las nuevas formas de delinquir a través de las tecnologías de información y la comunicación, se creó la Ley contra Delitos Informáticos y Conexos donde se regula el delito de estafa informática de manera autónoma". (Carranza, J.; Hernández, D. Universidad de El Salvador,2022).

3- " Con la clasificación del tipo penal de estafa informática, se logro determinar, que

este delito es distinto, al delito tradicional de estafa y se compone por varios verbos rectores, además es un delito de resultado, es doloso y tiene un elemento subjetivo distinto del dolo que es el ánimo de lucro, e mono ofensivo porque solo se protege el bien jurídico patrimonio" (Carranza, J.; Hernández, D. Universidad de El Salvador,2022).

4- Se concluye que el sujeto activo puede ser cualquier persona, el sujeto pasivo es indeterminado porque cualquiera puede ser víctima de este delito, es el nexo causal en el delito de estafa informática se caracteriza por la ausencia del engaño y el error ya que la obtención del patrimonio se da mediante la manipulación de las tecnologías de la información y la comunicación". (Carranza, J.; Hernández, D. Universidad de El Salvador,2022).

5- "La mayoría de los países regula el delito de estafa informática dentro del código penal y no es una ley especial, la pena es de prisión y multa". (Carranza, J.; Hernández, D. Universidad de El Salvador,2022).

6- "La Fiscalía General de la República no ha judicializado casos de estafa informática, los auxiliares del fiscal general no han sido capacitados sobre el tema de estafa informática". (Carranza, J.; Hernández, D. Universidad de El Salvador,2022).

7- "Existe ausencia de capacitación sobre delito de estafa informática en los jueces y magistrados tanto que algunos de ellos desconocen de la Ley Especial contra Delitos Informáticos y Conexos". (Carranza, J.; Hernández, D. Universidad de El Salvador,2022).

8- "El delito de estafa informática produce afectación política, social, económica y jurídica". (Carranza, J.; Hernández, D. Universidad de El Salvador,2022).

Con esta información de base, en cuanto al estudio sistemático de este flagelo de la Estafa Informática, estamos sustentando la importancia, relevancia, pertinente e

innovador del tópico a estudiar, ya que va en auge el mundo de la globalización y con ello la tecnología abre una puerta para mayores mecanismos de emplear o cometer un delito informático, y más concretamente el de Estafa Informática, es por ello que es sostenible el estudio y análisis de la temática para seguir indagando y dando a conocer los efectos jurídicos, alcances y consecuencias de dicho delito, ya que al conocer mejor todo el entorno y la magnitud del problema del tema, es que se pueden tomar acciones mas directas, encaminadas a fortaleces la justicia y a poder judicializar los casos y que tengan un proceso conforme a derecho.

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN.

3.1 Enfoque de la investigación.

Sobre el enfoque cualitativo Jorge Olvera (2014) plantea que:

El enfoque cualitativo de investigación consiste en conocer de cerca el objeto de estudio (un evento, una norma, la aplicación de un sistema jurídico, un fenómeno, una situación jurídica o una persona). El enfoque cualitativo habla de cualidades, de calidad particular de un determinado objeto de estudio. Desde este enfoque se realizan descripciones detalladas de una situación específica, de una persona determinada o un comportamiento. Se trata del análisis a profundidad de sólo un segmento de la realidad. Éste se basa más bien en la observación, en el contacto con el individuo, en una relación cercana con el problema de investigación. La investigación cualitativa ofrece al investigador un conjunto de técnicas especializadas para obtener información de índole interpretativa sobre un fenómeno, problema, persona o grupo.

En el método cualitativo, el investigador se aproxima a una situación cotidiana (jurídica, social) o a un sujeto que está presente en el mundo real y que se presenta como una fuente de información sobre sus propias experiencias, opiniones y valores. (p. 87).

Olvera García, Jorge, Metodología de la investigación jurídica: para la investigación y elaboración de tesis de licenciatura y posgrado, Unidad Autónoma del Estado de México, México, 2015.

3.2 Método:

El método en cuanto a su definición a seguir , en cuanto a su definición teórico conceptual, y el enfoque será el método Cualitativo, y con estudio de casos, ya que es el método científico de observación para recopilar datos no numéricos, sino, que recoge los discursos o acontecimientos existentes en torno al tema y realiza luego una interpretación rigurosa.

3.3 Tipo de estudio:

En cuanto al tipo de estudio en cuanto a su clasificación y alcance será no experimental, ya que se observaran los fenómenos o acontecimientos tal y como se dan en su contexto natural, para después analizarlos, por lo que se observarán situaciones ya existentes.

CAPÍTULO IV: TERMINOLOGÍA Y DOCTRINA

4.1. Glosario y sus definiciones

Ciberdelitos: Delitos Informáticos

Contrato criminalizado o contrato civil criminalizado: Pen. Contrato en que una de las partes actúa con el propósito de aprovecharse del cumplimiento de la otra parte contratante, sin intención de cumplir sus obligaciones.

Delitos Informáticos: Pen. Infracción penal cometida utilizando un medio o un instrumento informático

Estafa (convencional o simple): Pen. Delito que comete el que, con ánimo de lucro, utiliza engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno

Medios informáticos o Medios digitales: Son todas aquellas plataformas que se encuentran en internet. Generalmente, los medios digitales de comunicación, incluyen software, imágenes, vídeos, archivos, base de datos y sonidos. Entre otros.

Hipertexto: La narrativa digital surge y fluye en el hipertexto, en un soporte multimedia, con la utilización de diferentes códigos y lenguajes (textuales, gráficos, visuales, sonoros y audiovisuales). La interacción posibilita la intervención del usuario como emisor, productor, curador y distribuidor de contenidos, propios y ajenos.

Perjuicio patrimonial: En el delito de Estafa consiste en toda disminución en el patrimonio.

4.2. La estafa electrónica en el derecho comparado

En el presente apartado se hace una comparación de diversas legislaciones que regulan las estafas electrónicas u otra modalidad similar de fraude por medios informáticos con la finalidad de ilustrar las diversas concepciones legislativas del problema que conlleva la expansión de la tecnología y de la economía.

MÉXICO.

La criminalidad cibernética en México

A partir de 1999 hay legislación a nivel federal que sanciona los delitos informáticos en México , según la directora del despacho IT Lawyers, Ivonne Muñoz.

En opinión de la abogada especializada en ciberseguridad, el sector financiero es el que más ha trabajado en leyes especiales que se refieren a la comisión de este tipo de ilícitos.

Para Cynthia Solís, una de las socias de la firma legal especializada en derecho informático LEXINF, en líneas generales hay dos tipos de delitos informáticos: aquellos que tienen como finalidad destruir; alterar; modificar, o extraer información de manera no autorizada de los sistemas informáticos, y la del orden común que se comete a través de nuevas tecnologías.

En entrevista, Solís explicó que en la segunda clasificación entre el **phishing**, que jurídicamente es un concurso de delitos; es decir, diferentes crímenes que se cometen en un mismo momento. Por ejemplo, detalló que cuando una persona recibe una liga apócrifa con una alerta de su banco que dice que tiene un cargo no reconocido, le pide que entre a ese enlace con sus claves para revisarlo o rechazarlo.

El hecho de copiar o clonar la apariencia de una página web ya es un delito en materia de derechos de autor, pero lo que se busca realmente es cometer el delito de fraude: apoderarse de un bien a través de engaño o aprovechando el error de la persona. (360, 2023)

Ley de Instituciones de Crédito

Artículo 12 Bis.- " Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o extranjero:

i. Produzca, fabrique, reproduzca, introduzca al país, imprima, enajene, aun gratuitamente comercie o altere, cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

ii. Adquiera, posea, detente, utilice o distribuya cualquiera de los objetos a que se refiere el párrafo primero de este artículo

iii. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

iv. Altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

v. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo;

vi. Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada". (diputados.gob.mx, 2024)

Colombia

Criminalidad informática en Colombia

Uno de los más frecuentes modos de fraude en los últimos años ha sido por medio de las páginas web o plataformas digitales, lo que mantiene las alarmas encendidas entre los usuarios y las autoridades que enfrentan este tipo de delitos. Según un informe reciente de la central de información financiera TransUnion, se presentó una disminución de este fenómeno entre 2023 y 2022.

Sin embargo, en Colombia se ha registrado un alarmante incremento del 89% en los casos de fraude al consumidor a través de sitios web de citas en línea y foros, marcando el mayor aumento en este tipo de delitos comparado con otros sectores. Este preocupante fenómeno es seguido por un aumento del 46% en el fraude vinculado a juegos de apuestas deportivas en línea y un 28% en sitios de logística, de acuerdo con el análisis realizado por la central de información.

El fraude digital en la fase inicial de apertura de nuevas cuentas puede representar una especie de cambio de paradigma entre los estafadores. En lugar de utilizar tácticas tradicionales para acceder y comprometer cuentas existentes, están optando cada vez más por crear nuevas cuentas que pueden controlar ellos mismos", manifestó la directora de Soluciones de Fraude e Identidad Digital para TransUnion América Latina, Diana Martínez. (Infobae, 2024)

El Estado Colombiano, es pionero en la efectiva protección de las víctimas de estafas electrónicas o fraudes informáticos a través de una reforma que pretende proteger a las víctimas y que pone de manifiesto la responsabilidad por fragilidad de los sistemas informáticos de las instituciones bancarias frente a los delincuentes cibernéticos.

Bogotá D.C., julio 11 de 2023 (Prensa Senado). En Colombia, entrará a regir en los próximos días una ley que discutió y aprobó la plenaria del Senado, en el cierre del pasado período de sesiones ordinarias, que impedirá que las personas que hayan sido víctimas de estafas, de fraude digital, tengan que pagar deuda y demás consecuencias, que no les corresponde.

Esta ley llega en un momento en el que, según un estudio de Tendencias Globales de Fraude Digital elaborado por TransUnion, revelado en mayo pasado, en Colombia los casos de intentos de fraude digital crecieron de forma vertiginosa a un 134 %, mientras que a nivel mundial se registra un 52%. Según el reporte, tres de cada diez colombianos estuvieron expuestos a estos tipos de delitos.

Ante esta compleja situación, que afecta en particular a personas que fueron engañadas, se tramitó este proyecto de autoría del representante a la Cámara, **Duvalier Sánchez**, **Alianza Verde**, que recibió en el Senado un total apoyo, para permitir que por lo menos 40 mil personas que han sido víctimas de estafas digitales, puedan quedar exoneradas de pagos de productos, o créditos que nunca tomaron. (COLOMBIA, 2024).

LEY 1273 DE 2009

La ley 1273 del año 2009, aprobada por el congreso colombiano el día 5 de enero del año 2009 realiza una modificación al Código Penal Colombiano insertando el “ Título VII BIS denominado "De la Protección de la información y de los datos".

Se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Dicho cuerpo normativo, tipifica una serie de conductas entre las que destacan las siguientes:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. Artículo 269F.

VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Argentina

Criminalidad informática:

Entre abril de 2022 y marzo de 2023 fueron registrados **en la Argentina más de 35.000** ***ciberdelitos,*** un número que equivale a un aumento del 38% de los casos en comparación a los 12 meses previos, según se desprende de un informe realizado por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), que catalogó la situación como **"preocupante"**. A la vez, la UFECI notó una "consolidación" de este tipo de hechos tras la pandemia por ***Covid-19.***

La Unidad a cargo del fiscal general **Horacio Azzolin** presentó esos números en su informe de gestión 2023. El documento destacó un aumento en las modalidades de **fraude en línea, usurpación de identidad y secuestro de datos** (ransomware)[1] y un leve descenso en las maniobras asociadas a la compraventa de productos y estafas a través de servicios de billetera virtual.

La unidad especializada registró un incremento del 38,5% de los reportes recibidos, que pasaron de 25.588 a 35.447, **lo que equivale 2.241 reportes mensuales**. "En efecto, aun verificando un aumento año tras año, el porcentaje de crecimiento tendió a la baja luego del abrupto ascenso detectado en los primeros doce meses de la pandemia", se indicó en el documento.

Regulación penal:

El Código Penal Argentino, establece una gama de tipos penales cometidos por medios informáticos y los cataloga según el bien jurídico tutelado entre los bienes jurídicos tutelados destacan: a) delitos informáticos contra la integridad sexual; b) delitos informáticos contra la libertad; c) delitos informáticos contra la propiedad; d) delitos informáticos contra

[1] El ransomware, en informática, es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta. El ciberdelincuente toma control del equipo o sistema infectado y lo "secuestra" de varias maneras, cifrando la información, bloqueando la pantalla, etc.**Fuente especificada no válida.**

la seguridad pública que atentan contra los medios de comunicación; e) delitos informáticos contra la administración pública.

Los delitos informáticos contra la propiedad regulados en el código penal Argentino son los siguientes:

- la estafa mediante el uso de tarjeta magnética o de los datos de la tarjeta;

- la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos;

- el daño informático, que consiste en alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos; vender, distribuir, hacer circular o introducir en un sistema informático, cualquier programa destinado a causar daños. La pena es mayor en caso de dañar datos, documentos, programas o sistemas informáticos públicos; causar daño en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público. (Argentina, 2024).

Estados Unidos

Más de US $10.000 millones en pérdidas por estafas en línea fueron reportadas al FBI en 2022, la pérdida anual más alta en los últimos cinco años, según un nuevo informe del Buró de Investigaciones.

El aumento de más de US $3.000 millones en informes de fraude en línea de 2021 a 2022 fue impulsado por el hecho de que casi se triplicaron los informes de fraude de inversión en criptomonedas, dijo el FBI en su Informe anual de delitos en Internet.

El informe reúne una amplia variedad de denuncias de fraude, desde estafas de marketing hasta ransomware[2], y es una métrica para los legisladores de EE.UU. para medir cuánto le cuestan a la economía estadounidense la piratería y otros esquemas. (Sean Lyngaas, 2023)

En cuanto al concepto de "delito cibernético", cabe señalar que la legislación estadounidense es pionera en la materia, y es la que acuñó el concepto (cybercrime). Ésta utiliza una acepción amplia del mismo, la que comprende tanto aquellas situaciones en que el elemento informático se encuentra en el objeto de la conducta penada (vg. intromisión ilegal a bancos de datos), como aquellas en que dicho elemento es el medio para realizar un fin ilícito (vg. estafa vía Internet).

Por su parte, de acuerdo a Naciones Unidas, los llamados delitos informáticos, o delitos cibernéticos, en sentido estricto, son aquellos que implican un "comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos.

De esta manera, el concepto de cibercrimen (o ciberdelitos) en sentido amplio, abarca tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución sólo es posible gracias a la existencia de dichos medios. Esto implica que la respuesta a este tipo de criminalidad apele tanto a la legislación general como a leyes especialmente diseñadas para combatirla, sin perjuicio de que se critique la inadecuación de la legislación basada en la jurisdicción estatal para perseguir un fenómeno de alcance global.

Ciberdelitos fraude y acceso ilegal:

Sin perjuicio del desarrollo casuístico respecto de casos de fraude, acceso ilegal y vandalismo informático, en 1984 se dictó la Ley de Fraude y Abuso Informático (CFAA, por sus siglas en inglés). Esta normativa federal tipificó siete conductas relativas a acceso ilegal

[2] El ransomware, en informática, es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta. El ciberdelincuente toma control del equipo o sistema infectado y lo "secuestra" de varias maneras, cifrando la información, bloqueando la pantalla, etc.**Fuente especificada no válida.**

a computadoras, aunque sólo se refiere a "ordenadores protegidos", esto es, aquellos utilizados por instituciones financieras, el gobierno federal, o usados en comercio o comunicaciones entre estados de la Unión o terceros Estados. Ahora bien, la noción de ordenadores protegidos es suficientemente amplia como para comprender todo computador conectado a Internet, pues incluye aquellos utilizados para la comunicación interestatal.

Usurpación de identidad y fraude:

En 1998 se adoptó la Ley de Usurpación de Identidad. Conforme a ésta, es un crimen federal utilizar ilegalmente un medio de identificación de otra persona para cometer una actividad ilegal.

Las penalidades pueden llegar hasta los quince años de prisión. En casos vinculados a terrorismo, la misma puede llegar a veinticinco años.

Fraude y dispositivos de acceso:

La ley federal considera como delito actividades que utilicen de un modo ilegítimo "dispositivos de acceso" tales como tarjetas, códigos, números seriales y contraseñas, para obtener dinero, bienes, servicios u otros valores de modo fraudulento.

La Ley USA PATRIOT (por sus siglas en inglés), dictada en 2001 como reacción a la amenaza terrorista, extendió la aplicación de esta ley más allá de la jurisdicción de los EE.UU, siempre que la comisión del delito incluyere un dispositivo emitido en el país y que el imputado hubiere transportado, enviado o almacenado en dicho país algún elemento para cometer el delito. (CHILE)

España

El **robo de identidad** es uno de los principales delitos cibernéticos que ocurren con frecuencia en España. Con los avances tecnológicos y la dependencia cada vez mayor de plataformas digitales, se ha vuelto más fácil para los delincuentes suplantar la identidad de

otras personas y cometer crímenes utilizando identidades falsas. Esta **estafa digital** puede tener graves consecuencias para las víctimas, como la pérdida de sus ahorros o daños a su reputación.

¿A qué se refiere la suplantación de identidad?

La suplantación de identidad, o robo de identidad, se ha convertido en un delito cibernético cada vez más prevalente tanto en España como en todo el mundo. Esta práctica consiste en que **un individuo se hace pasar por otra persona, usando su información personal y financiera con el fin de cometer diversos tipos de fraudes y actividades ilícitas.**

Las consecuencias de ser víctima de suplantación de identidad pueden ser devastadoras. Los delincuentes pueden llevar a cabo una serie de actividades ilegales en nombre de la víctima, tales como realizar compras fraudulentas, acceder a cuentas bancarias, solicitar préstamos o créditos, sustraer información confidencial, entre otros delitos.

En esta línea, **la suplantación de identidad on-line ha aumentado** debido a las crecientes transacciones on-line y **avances tecnológicos**. Los delincuentes obtienen información personal a través de estafas como el *phishing* y el robo de datos en brechas de seguridad.

Este delito es castigado por leyes y regulaciones, y es importante tomar precauciones como proteger contraseñas y datos personales, así como utilizar sistemas de protección como antivirus y *firewall*. **En España, la suplantación de identidad se considera un delito de estafa según el Código Penal, y los culpables pueden enfrentar penas de prisión y multas**. (CENTRAL, 2023)

China

La Sociedad de Internet de China (ISC, siglas en inglés) emitió hoy una advertencia sobre el creciente uso de tecnologías de síntesis profunda, como el cambio de rostro y voz

con inteligencia artificial (IA), que está dando lugar a "un incremento en actividades ilegales como el fraude y la difamación".

El comunicado de la ISC destaca un caso de fraude en la red de telecomunicaciones destapado por las autoridades de Baotou, ciudad de Mongolia Interior (norte), donde los perpetradores utilizaron tecnología de IA para sintetizar voces y cambiar rostros con el fin de cometer estafas.

Los delincuentes usaron esta tecnología para falsificar la voz de una persona en concreto a través de la síntesis de sonido, cambiar rostros utilizando IA, pretender ser una persona específica y hacer videollamadas con otras personas en tiempo real, con el objetivo de ganarse la confianza de la víctima y cometer fraude.

Ante este escenario, la ISC enfatiza la importancia de adoptar medidas de seguridad personal frente a las nuevas formas de estafa que utilizan tecnología de IA, como proteger la información personal, evitar la descarga de software desconocido y gestionar cuidadosamente el círculo social en línea.

Asimismo, se recomienda a las personas realizar múltiples verificaciones al realizar transferencias de dinero y no confiar únicamente en la comunicación por mensajes o llamadas telefónicas.

En respuesta a esta problemática, la ISC, una organización no gubernamental china compuesta por 140 miembros de la industria china de Internet, incluidas empresas privadas, escuelas e institutos de investigación, pide "autodisciplina" en la industria y "trabajar en la prevención y gobernanza de las telecomunicaciones".

El pasado 17 de mayo, el Ministerio de Industria y Tecnología de la Información de China (MIIT, siglas en inglés) anunció la creación de un comité y un grupo de expertos en ética de ciencia y tecnología, con el objetivo de establecer un sistema de administración único para abordar cuestiones éticas en el campo de la IA.

Además del MIIT, otras autoridades chinas también han tomado medidas para regular el uso ético de este campo.
La autoridad de ciberespacio de China emitió recientemente un borrador de regulación de contenido para la IA, expresando su respaldo a la innovación y aplicación de algoritmos y marcos del sector, así como a la garantía de una competencia justa.

Asimismo, las plataformas de redes sociales chinas están marcando el contenido generado por IA para prevenir disputas y ayudar a los usuarios a distinguir entre elementos virtuales y reales, en una muestra más del férreo control ejercido por el gigante asiático en la red.

El Gobierno chino anunció a principios de año que continuará brindando apoyo a la "industria estratégica emergente" de la inteligencia artificial para aprovecharse de sus beneficios, poniendo a ChatGPT como ejemplo de crecimiento. EFE (swissinfo.ch, 2023)

4.3. Análisis de delitos informáticos.

Definición doctrinaria:

Es importante visualizar o recabar la forma de analizar por otros estudiosos del derecho este importante tema, que nos ha llevado a este análisis, es por eso que presentamos algunos de las definiciones que más nos llamaron la atención, las cuales son las siguientes:

De manera general para poder entrar en el tema, debemos partir de lo que se consive como la ciberdelincuencia por medio de los delitos informaticos; es por ello que retomamos lo que establecen los autories Marcelo Huerta y Claudio Líbano que definen como delitos informáticos a "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter

patrimonial, actúe con o sin animo de lucro". Esta definición tiene la ventaja de ser bastante amplia en donde enmarca varias tipologías de delitos informáticos dentro de los cuales está la estafa informática que es la que estudiaremos en párrafos posteriores.

Ahora bien, luego de establecer una definición general, entramos en materia, visualizando lo que nos dicen sobre la estafa informática, autores como Rosso Perez, Manuel Enrique, define la Estafa informática como " la producción de un daño patrimonial cuantificable mediante un comportamiento externo, impropio de un proceso automatizado informático, que altera los datos gestionados por este, con ánimo de lucro y en perjuicio de un tercero".

De la misma forma lo establece el autor Gutiérrez Francés, en el art. 248 apartado dos, decía "También se considera reos de estafa los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero."

Y en la legislación del Código Penal Alemán se establece lo siguiente: Estafa por Computador "Quien con el propósito de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que el perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado d datos, o de otra manera por medios de la influencia no autorizada en el desarrollo del proceso, (…)"

También traemos a colación la doctrina del tribunal Supremo que menciona un punto muy importante: " en efecto, los aparatos electrónicos no tienen errores como los exigidos por el tipo penal tradicional de la estafa, es decir, que en sentido de una representación falsa de la realidad. El aparato se comporta según el programa que lo gobierna y, en principio, sin "error". Esta misma doctrina pone de manifiesto que el tipo de la estafa informática admite diversas modalidades comisivas, "bien mediante la creación de órdenes de pago o transferencias, bien a través de la manipulación de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia."

Y reforzando el mismo orden de ideas, solo con algunas variaciones, tenemos al autor Chileno Gustavo Balmacea Hoyos el cual menciona que "…debería de efectuarse una lectura alternativa del tipo de Estafa Clásico, con el objetivo de viabilizar la inclusión en su seno de los comportamientos que se contemplan en la Estafa Informática. Así su expresa tipificación solamente representaría una interpretación auténtica de los límites del delito de Estafa Tradicional."

En esta última opinión jurídica de este autor chileno, lo hace en el contexto que en ese país no existe una tipificación exclusiva de estafa convencional sino que en esa legislación lo que se expone son una serie de ejemplos de los que se consignarán como estafa simple, por lo que es demasiado general, para poder determinar los límites entre una y otra estafa, y sus modalidades o variantes, hasta donde es una y hasta donde iniciara otra modalidad de este delito. (Revista de Derecho y Ciencias Penales, Universidad San Sebastián, Chile)

Aspecto legal de estafa en El Salvador. (estafa convencional):

Art 215 C. P Estafa " el que obtuviere para sí o para otro un provecho injusto en perjuicio ajeno, mediante ardid o cualquier otro medio de engañar o sorprender de buena fe, será sancionado con prisión de dos a cinco años si la defraudación fuere mayor de doscientos colones (…)

El Elemento más importante en la norma es el elemento Engaño o Ardid para que pueda configurarse el delito de estafa.

Aspecto legal de estafa informática en El Salvador, la cual se visualiza así:

Art. 10 Ley Especial Contra los Delitos Informáticos y Conexos. Estafa Informática " 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…" (el subrayado es nuestro)

Análisis general de la estafa informática:

En un análisis que realiza la Fiscalía General de la República a través de su escuela de capacitación y en colaboración de ONUDC en donde se realiza una línea de pensamiento muy atinada y que compartimos, en cuanto a los elementos del tipo penal de la estafa de forma convencional, ya la estafa por medios electrónicos; ya que se atañe a que si una determinada conducta defraudatoria es susceptible de ser tratada jurídicamente bajo el delito de estafa, a la que se le calificara como común, se requiere principalmente, la comprobación de si ha existido un engaño (y consiguiente error) que sufre una persona física como consecuencia de la confabulación engañosa elaborado por otra. Tal y como se estableció en párrafos arriba mencionados.

En cuanto a la otra modalidad de estafa que es la informática, se resalta la importancia de identificar cual es el elemento determinante, y en este caso según el análisis realizado por la escuela de capacitación fiscal, es la manipulación informática o artificio semejante. En ese entendido, ponemos en contraposición el elemento engaño (estafa común) y el elemento manipulación informática (estafa informática) término que se acuña al art 248.2 del Código Penal de España, año 1995 según lo retoma este estudio de análisis que estamos en algunos de acuerdo y concordancia, en algunos puntos del análisis, puntos como este, en el cual se estableció la palabra "Manipulación Informática", siendo retomada más adelante por El Salvador en la disposición legal antes citada, sin embargo se quiso incorporar con matices, siendo realmente insuficiente una manipulación por medios informáticos para poder establecer un tipo de estafa.

Se analiza también el hecho de los elementos preparatorios que podrían entrar en delitos en el comercio mercantil como se señaló al principio, pero pueden quedar subsumidos estos tipos de manipulación para obtener un fin último que es estafar por medios electrónicos, en ese sentido podríamos hablar de la insuficiencia de por ejemplo manipular para obtener datos personales de la víctima, suplantando su identidad, y ser constitutivo de delito pero, realmente podría verse como un acto preparatorio subsumido en el fin último de estafar a la

víctima, violentando su patrimonio, sin embargo, se menciona que la disposición salvadoreña además de ser insuficiente, se mantiene fuera de la realidad y actualización del tipo penal, ya que esta como resabio siempre el engaño y el ardid, situación que para ellos es insostenible ya que las máquinas no cometen errores, ni pueden ser engañadas.

En ese orden de ideas se puede extraer elementos importantes como que para que exista esta situación delictiva, deben existir sujeto activo y sujeto pasivo de la acción; debe existir un ardid o engaño, sin embargo en cuanto al medio o forma de realizarlo en esta caso en análisis se establece el elemento de utilización de medios tecnológicos, como operaciones de comercio electrónico, y se menciona que dentro de la configuración común, debe existir una relación entre comprador y vendedor anteriormente acreditada, de la cual cuando ya se tiene prefijado esa determinación, uno de los dos puede salir engañado o inducido a error. Sin embargo en el delito de estafa electrónica se rompe la tipicidad común de la estafa convencional, ya que a pesar de no tener una interacción física, si se puede establecer que por medio de algún operación o artificio informático, como Facebook, Messenger, WhatsApp, Instagram, tik tok entre otros, se puede entablar esta calidad de vendedor y comprador y ejecutar la operaciones de comercio, inclusive existen páginas dedicadas exclusivamente dentro de las redes sociales a compra venta de bienes y servicios, por ejemplo Marketplace en Facebook, OLX, Mercado Libre, etc.

Siguiendo ese criterio supra estipulado, la diferencia sustancial radica en la ausencia de engaño y error, elemento esencial o sinecuanon para configurar el delito de Estafa del 215; sin embargo el elemento tipo de la estafa informática art 10 LEDIC radica en que el autor se vale de "operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos…" esto para poderse configurar como estafa informática.

Concluyendo esta idea, que el debate se encuentra que si en el delito de estafa informática existe o no puede existir engaño o ardid, y si la manipulación informática es suficiente para configurar este delito, o si existen más elementos esenciales.

4.4. Bien jurídico o bienes jurídicos protegidos:

Según la autora Gutiérrez Frances (1994) menciona que el bien jurídico protegido o tutelado en los delitos informáticos en general, se pone en peligro y se vulneran varios bienes jurídicos tutelados, es por eso que se consideran pluriofensivos, ya que se puede ver en el plano de manera conjunta ya que la información se encuentra de manera general (información, almacenada, tratada y transmitida. Mediante los sistemas de tratamiento automatizado de datos), y en el plano de una concatenación se dice que todos los demás bienes afectados a través de este tipo de delitos informáticos, como por ejemplo la intimidad, indemnidad sexual, patrimonio, datos personales, etc. Bajo este criterio de la autora, la información es un bien jurídico como de interés colectivo tutelado penalmente de forma conjunta con bienes de los particulares, siendo ambos situados en la misma línea de ataque, por lo que hay una relación entre el derecho a la información como bien colectivo y los derechos individuales que pueden verse afectados. Es decir, que el primero es un paso previo, o un medio para poder lesionar o poner en peligro los derechos individuales. (el subrayado es nuestro)

En este último párrafo se establece el núcleo de la importancia del estudio y el análisis del Derecho Penal económico a través de delitos como este, que inicialmente afectan a una colectividad, pero que en el fondo también merman los derechos individuales de las personas, y es por ello que al retomar este delito informático como la estafa informática, se puede dilucidar que primeramente los datos o información personal o ese banco de datos es vulnerado, para poder lesionar directamente bienes jurídicos tutelados como el patrimonio, honor, intimidad, etc, en donde en este caso en concreto de la estafa informática, el patrimonio y el valor económico que representa, está en juego de ser vulnerado o de vulneración concreta.

En ese orden de ideas podríamos poner dos ejemplos de elementos diferentes y complejos que conllevan a preguntarnos si se utilizará el mismo tipo penal o no, para estos casos a continuación:

Ejemplo1: Sujeto A hace un anuncio de un artículo X, lo ve en internet o redes sociales la víctima B quiere comprar ese artículo y manda por transferencia el coste o precio

del artículo que le parece legal y existente ; el sujeto A recibe la transferencia voluntaria de la víctima B y al recibir el dinero en su cuenta lo saca de su cuenta bancaria, pero no manda el artículo X, o puede mandarlo pero no de lo que se había convenido comprar y vender. En éste caso se podría decir que se indujo a engaño a la víctima, y ésta realizó voluntariamente la trasferencia pero de forma engañada o errara de una realidad diferente, creyendo que recibirá el artículo que ha comprado en línea.

Ejemplo 2: Sujeto A manda correo a Víctima B, diciendo que necesitan que actualice sus datos del banco, a lo que la víctima hace click en el link que se le mandó por A, y en ese momento sus datos personales y bancarios están al descubierto, el sujeto A, luego de hurtar los datos, suplanta la identidad de la víctima B y retira dinero o se transfiere individualmente de la cuenta de la víctima B, dirigido la cuenta de A. En este caso no existe engaño en la víctima en cuanto a la transferencia de dinero de una cuenta a la otra ya que el sujeto A realizar todo el procedimiento individualmente a su favor, es decir el propio sujeto activo realizó esta operación informática ilegal para su beneficio, sin consentimiento de la víctima. Sin embargo hay otros bienes jurídicos vulnerados, ya que para llegar a la acción última del perjuicio patrimonial económico, vulnero por medio de otras acciones independientes o transitorias, que constituyen otros delitos informáticos y que por ende vulneran varios bienes jurídicos, es por ello que se llama que estos delitos son "PLURIOFENSIVOS" tal cual como lo es la característica esencial de los Delitos del Derecho Penal Económico.

4.5. Elementos objetivos del tipo penal:

Según el análisis que realizan en la escuela Fiscal, establecen que los elementos Objetivos son los siguientes:

a) **Sujeto activo :**

Según el artículo que hace referencia a la Estafa Informática establece como sujeto activo **"El que",** de lo que se puede determinar que establece de forma genérica el sujeto activo, es decir cualquier persona natural que realice directa o indirectamente con el accionar delictivo, sin embargo a pesar que esta definición que nos da el articulo 10 LEDIC, es muy amplia y en el que deberíamos entender cualquier persona con conocimiento o no técnico que realice dicho accionar, es necesario

considerar que para poder llevar acabo un accionar informativo de esta índole, se debe de tener un conocimiento poco más superior que la mayoría de las personas convencionales, que hacemos uso de una computadora, un teléfono o un aparato informático, por lo que tener un conocimiento previo del sujeto activo en cuanto a la tecnología y sus "agujeros negros" para poder entrar, salir, programar, recabar, recopilar y efectuar el accionar defraudatorio, es importante destacarlo ya que si bien es cierto que el articulado no lo establece como una característica especial o un perfil profesional o técnico para tipificar al sujeto activo, si es preponderante mencionar que este sujeto activo tiene algún conocimiento superior al del conglomerado de la población que usa sus computadoras y teléfonos inteligentes para ver e interactuar con redes sociales, mandar correos de forma convencional y simple.

Esta idea la acota muy certeramente la autora Chinchilla Sandi (2004) estableciendo lo siguiente: "no obstante no sea necesario que el autor posea una condición especial para calificar dentro del supuesto, hay que considerar que este tipo de infractores tiene capacidades intelectuales un poco más arriba del promedio, por lo que se les califica en el lenguaje técnico como: Hacker, Cracker, Phreaker, entre otros calificativos".

Esto engloba a que el sujeto activo puede ser desde una persona menor de edad y sin un alguna posición privilegiada en la sociedad o en una empresa, hasta las personas que tienen posición especial en una empresa, que tiene claves o cuentas a su disposición o bien que tiene algún nivel de jerarquía y poder en la sociedad, empresa, economía, etc; siempre y cuando tengan esta capacidad intelectual y técnica de adentrarse en el mundo de la tecnología con propósitos defraudatorios.

Otro punto importante de destacar es que debe ser realizado por una Persona Natural o física, y no por una Persona Jurídica, ya que actualmente en nuestro país no se reconoce plena y totalmente el accionar de una persona jurídica propiamente dicha, es por ello que en el tipo penal de este delito debe ser una persona natural o llamada persona física la que realiza el accionar; a diferencia de otros países como por ejemplo España.

Como se menciona en el desarrollo del tema, este delito de estafa informática es un delito de resultado, es por ello que el sujeto activo debe tener la obtención de un provecho para él o para un tercero, en perjuicio ajeno obteniendo un beneficio patrimonial directo.

b) Sujeto pasivo:

- Es la persona o personas titular o titulares del derecho patrimonial económico afectado, aquella persona que directamente a sufrido un perjuicio patrimonial que le causa disminución en su esfera patrimonial.

- Aquellas personas naturales que no son directamente titulares del derecho patrimonial económico, pero que son vulneradas por ser los titulares de la información o de los datos extraídos o violentados, también los titulares de los programas objeto de la acción delincuencial, además de los equipos, y sistemas afectados para alcanzar el fin ulterior; aunque no sufran afectación patrimonial económico efectivo, también se les ha vulnerado en sus derechos y de manera indirecta se podría mencionar, datos informatizados con valor contable. En este punto es importante destacar también que cabe la posibilidad de evidentemente también ser afectado una persona jurídica, como bancos, gobiernos, empresas, etc. A diferencia del sujeto activo que solo se refiere y puede ser a una persona física.

- La sociedad en general también sufre afectación en cuanto a la información, la seguridad jurídica de todos los datos expuestos y los sistemas por los que se procesa y transfiere de forma legítima esta información, que se han utilizado de manera ilegal.

c) Conducta típica:

Se establece como un delito de resultado, y de conducta meramente Dolosa (no cabe la modalidad culposa) donde lo que busca el sujeto activo es el provecho o

beneficio patrimonial o no patrimonial (en el caso de los sujetos pasivos colaterales) para si o para un tercero.
La conducta típica al ser realizada, se toma como configurada o consumada ejecutando las siguientes formas de acción en un sistema que utilice las Tecnologías de la Información y la Comunicación (TIC´s).

Realizando un uso indebido de esa tecnología de la información y la Comunicación, valiéndose de cualquier forma o medio de manipulación en el sistema informático o cualquiera de sus componentes, datos informáticos o información importante en ellos contenida. También conseguir insertar instrucciones falsas o fraudulentas en sistemas informáticos o información que contenga estos.

- **Manipulación:**

  En este punto, es importante esa actividad que se realiza por el sujeto activo, para modificar o alterar de alguna forma el funcionamiento o procesamiento de datos o información de una manera determinada. Es por ello qué así como lo sostiene el magistrado y doctor en Derecho José Antonio Choclan Montalvo, que la Manipulación es toda acción que suponga intervenir en el sistema informático alterando, modificando u ocultando los datos que deban ser tratados automáticamente o modificando las instrucciones del programa, con el fin de alterar el resultado debido de un tratamiento informático y con el ánimo de obtener una ventaja patrimonial.

  En ese sentido este elemento es totalmente necesario para determinar si existe tipicidad en la conducta, así como en la estafa convencional es necesario el Ardid o el Engaño para inducir a error a la víctima, en este caso en la estafa informática es necesario establecer que existió una manipulación dolosa de alguna medida que resultó en perjuicio patrimonial del sujeto pasivo, en donde sin esa manipulación el resultado hubiese sido diferente. Por lo que que es ahí la importancia de este accionar de manipulación de los medios informáticos para inducir a error a la víctima o bien que datos y procesos

normales sean sistematizados de manera diferente de en perjuicio pecuniario del o los afectados.

- **Transferencia no consentida de activos patrimoniales en perjuicio de un tercero.**

  Según el autor que se citó en párrafo supra, Choclan Montalvo, establece una línea de pensamiento muy interesante, el cual plantea que: 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 tercer. Por lo tanto, no tiene cabida la disposición inducida por error a una persona humana en detrimento de su propio patrimonio, sino, la transferencia realizada por una máquina sin intervención de la persona humana.

  Ahora bien, en cuanto a nuestro país El Salvador, en la norma jurídica no contempla taxativamente la transferencia no consentida de activos patrimoniales en perjuicio de un tercero, ya que en este caso en concreto el resultado de la manipulación de los sistemas informáticos o procesos, es individualmente es que recae en la máquina, computadora, cajero, kiosko o lo que se utilice como receptor de esa manipulación, para que sin el consentimiento de la víctima, la máquina transfiera patrimonio económico en detrimento de la víctima.

D**) Circunstancias agravantes contenidas en el tipo penal:**

- El Art 10 La Ley Especial Contra los Delitos Informáticos y Conexos: "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."

- Asimismo, regula como circunstancias agravantes, 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, 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. Sancionándolo con una pena de 5 a 8 años.

4.6. Elementos subjetivos del tipo penal:

A) El dolo:

Es ese accionar del sujeto activo de querer y su intención de provocar un daño o un perjuicio en el sujeto pasivo afectando uno o varios bienes jurídicos. En este caso específico es ese conocimiento de causa de querer manipular a través de medios tecnológicos o artificios informativos para producir un daño o perjuicio económico de disminución del mismo, que sufre el sujeto pasivo o un tercero.

También se puede definir el Dolo como lo establece el análisis jurídico de la ley especial contra los delitos informáticos qué es "ese conocimiento de manipular o influir en el ingreso, procesamiento o resultado de los datos de un sistema que utilice las TIC¨s, con la finalidad de obtener o procurar un beneficio patrimonial indebido para sí o para otro, mediante transferencia no consentida de activos patrimoniales en perjuicio de un tercero, y la voluntad de realizar esa conducta."

B) **Ánimo de lucro:** se define como la intención de obtener un beneficio económico que se permite en los delitos dolosos.

La Real Academia Española lo refiere como "lucro" alude a la ganancia o al provecho que se saca de algo.

También se define en el diccionario Panhispánico del español jurídico, lo referente al delito de estafa y este elemento subjetivo del ánimo de lucro, que no es más que el propósito de obtener una ganancia económica o de poseer o disponer de una cosa con valor económico.

En este enfoque, se debe obtener la incorporación de lo estafado por los medio ya establecidos informáticos, sustrayendo de alguna manera del patrimonio del sujeto pasivo patrimonio económico, en detrimento de este, y pasándolo o adhiriéndose a su propio patrimonio para disponer de él enteramente.

Según la autora Selena Murriel Escobar estudia de la siguiente manera lo relativo a la importancia del ánimo de lucro en el delito de Estafa que consiste en la ventaja patrimonial que obtiene el autor con propósito de la apropiación de una cosa con valor económico, es el beneficio del sujeto activo al haber cometido el delito, la contrapartida del perjuicio sufrido por la víctima.

El sentido económico del lucro en la estafa es evidente en cuanto se entiende que es la contrapartida del daño patrimonial; sigue mencionando la autora, que el Tribunal Supremo (español) considera la ventaja patrimonial como cualquier utilidad y ventaja, pero no resulta esencial que se concrete en un determinado valor económico, por ello lo estima como cualquier ventaja. Comprende beneficio propio o a favor de un tercero, también han vislumbrado otra forma de lucro; se excluye la comisión por imprudencia, ya que el ánimo de lucro reafirma el dolo, y el objetivo del autor es obtener una ventaja patrimonial correlativa como contrapartida del perjuicio típico ocasionado aun cuando no sea equivalente.

Es muy importante poder visualizar que el ánimo de lucro reafirma la voluntad de querer obtener un perjuicio en el patrimonio económico del sujeto pasivo, es por eso que al igual que la legislación Española, en nuestro país no existe en los elementos del tipo comisión por culpa o imprudencia tal y como lo refiere la autora, porque es

incompatible con este elemento de ánimo de buscar lucrarse como fin último de su accionar o su camino del delito, desde sus actos preparatorios está presente el fin ulterior de disponer de patrimonio ajeno para poder sacar provecho para sí o para terceros de ese perjuicio económico. Por lo que entre el dolo y el ánimo de lucro hay una relación directa según nuestro criterio.

En El Salvador, los elementos subjetivos del delito en comento son el dolo y el ánimo de lucro como ya lo establecimos en este análisis, en donde el legislador establece en la norma jurídica ese elemento de provecho ilícito para si o para un tercero, es por ello que debemos entender que es parte de los elementos esenciales del tipo, a diferencia de la normativa española donde si bien es cierto es un elemento sobresaliente en los delitos de estafas y defraudaciones, también es sabido que el ánimo de lucro no es un elemento exigido como elemento subjetivo del tipo penal, a diferencia de la norma jurídica de nuestro país.

CAPÍTULO V: NUEVAS MODALIDADES

5.1. Las nuevas modalidades de estafa en la época posterior a la pandemia del COVID-19 en El Salvador

El ser humano depende de sí mismo para subsistir, sin embargo, necesita de los demás para poder alcanzar el desarrollo. Esa premisa nos indica que la subsistencia es un acto aislado, pero el desarrollo depende de las relaciones interpersonales.

Desde inicios de la humanidad el ser humano ha subsistido por sus propios medios para conseguir refugio y alimentación pero ha sido la convivencia con sus semejantes la que ha desarrollado sus habilidades para prosperar.

El comercio entre seres humanos es un ejemplo de prosperidad ya que implica un intercambio de bienes o servicios donde la parte que solicita el bien o servicio paga un precio por lo solicitado y la otra parte que lo proporciona recibe el pago acordado, con ese pago acordado puede adquirir bienes o servicios de otro y seguir la secuencia económica.

Esa relación comercial durante la historia se ha visto marcada por prácticas fraudulentas que van en detrimento del patrimonio del afectado y al ser realizadas en masa, a la economía.

Para Daniel Pablo Carrera "La presencia del dinero en la conciencia del hombre actual estimula al máximo su energía y lo ha hecho evolucionar, pero en un sentido especulativo y pragmático, calculador e interesado. (CARRERA, 2004)

Para el autor citado, el dinero tiene un efecto de estimulación en el ser humano que genera la evolución del hombre poniendo sus intereses por encima de los demás. Lo que da origen al delito derivado de los negocios y al delito que se pretende lucrar de los negocios, la primera forma delictiva se caracteriza que surge de la relación comercial (fraudes, estafas o apropiaciones indebidas) y el segundo no que surge de la relación comercial pero se beneficia de las actividades de comercio o de las ganancias generadas (hurto, robo, extorsión, etc.).

Con el avance de la tecnología y las nuevas formas de comunicación social, el comercio electrónico ha tenido un auge importante como una forma de generar dinero a través de la distribución y comercialización de productos a través de plataformas electrónicas,

algunas de ellas creadas específicamente para el comercio y otras para el ocio y entretenimiento que también generan espacios de negocios.

5.2. Ley de delitos informáticos en El Salvador

Por Decreto número 260, emitido por la Asamblea Legislativa de El Salvador del día cuatro de febrero de dos mil dieciséis, publicada en el Diario Oficial número 40, tomo 410 del 26 de febrero de dos mil dieciséis; se aprobó y publicó la ley de delitos informáticos como un cuerpo normativo de índole penal con la finalidad de proteger una serie de bienes jurídicos que si bien es cierto, algunos ya estaban protegidos por el código penal vigente, era necesario ampliar su margen de protección.

Es de hacer notar los fundamentos que tuvo el legislador para la aprobación de la referida ley, lo que se consignan en cada uno de los considerandos, de los que vale la pena resaltar los considerandos III Y IV, que literalmente dicen:

"III.- Que en la actualidad, los instrumentos electrónicos por medio de los cuales se envía, recibe o resguarda la información, han adquirido una especial relevancia, tanto a nivel internacional como nacional, para el desarrollo económico, político, social y cultural del país; por lo que se vuelve prioridad del Estado, proteger dicha información, ya que al no protegerla se atenta contra la confidencialidad, integridad, seguridad y disponibilidad de los datos en general.

IV.- Que esta diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación, no se encuentran suficientemente reguladas en nuestra normativa penal vigente, generando una impunidad para quienes cometen estos tipos de delitos; en consecuencia, resulta necesaria su tipificación y la adopción de mecanismos suficientes para facilitar su detección, investigación y sanción de estos nuevos tipos de delitos." (SALVADOR, portal transparencia.pgr.gob.sv, s.f.)

De los fundamentos del Legislador hay que destacar algunas ideas importantes, en primer lugar la relevancia adquirida por las tecnologías de la comunicación en la sociedad, tomando en consideración que dicha ley fue emitida en el año dos mil dieciséis, considerándose un cuerpo normativo novedoso para aquella época.

En segundo lugar la incidencia en el desarrollo político, económico y social de los instrumentos electrónicos utilizados para comunicarse, entendiendo el concepto de instrumento electrónico en sentido amplio, que sin embargo, será desarrollado más adelante.

En tercer lugar, que la regulación penal vigente en aquella fecha era insuficiente para regular los delitos informáticos lo que podría generar impunidad en las actividades delincuenciales por medios electrónicos.

El legislador establece un concepto de delito informático como en el artículo 3 letra a) de la ley, definiéndolo de la siguiente manera: "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" .

El concepto establecido por el legislador de delito informático es bastante limitado y hasta cierto punto ambiguo, dejando una serie de vacíos interpretativos que pueden llegar a comprometer los principios de legalidad y por ende de seguridad jurídica, por lo que el concepto general de delito informático refiere una descripción más precisa y detallada.

El convenio sobre la Ciberdelincuencia denominado comúnmente "Convenio de Budapest" del 23 de noviembre de 2001, hace una clasificación de delitos comunes cometidos por medios electrónicos y delitos informáticos, haciendo mención que los Estados parte de dicho convenio deben hacer una revisión de su legislación para evitar tipificar conductas que ya están tipificadas o modificar las existentes, así lo expresa el título 2, artículo 89 del convenio citado:

"Título 2 - Delitos informáticos

79. Los Artículos 7 a 10 se refieren a los delitos comunes que se cometen frecuentemente mediante la utilización de un sistema informático. Estos delitos comunes ya han sido tipificados como delitos por la mayoría de los Estados, cuyas leyes existentes pueden o no ser lo suficientemente amplias como para abarcar situaciones relacionadas con las redes informáticas (por ejemplo, las leyes existentes sobre pornografía infantil de algunos Estados pueden no abarcar las imágenes electrónicas). Por lo tanto, a la hora de aplicar estos artículos,

los Estados deben examinar sus leyes vigentes para determinar si se aplican a situaciones en que estén involucradas redes y sistemas informáticos. Si los delitos existentes ya abarcan dicha conducta, no existe ninguna obligación de introducir enmiendas a los delitos existentes o de establecer nuevos delitos[3].” (EUROPA, 2001)

Es conveniente identificar de forma clara lo que se entiende por delito informático. Existen diversas definiciones respecto; un ejemplo es la definición de Camacho Losa, citada por Leyre Hernández, quien considera como delito informático: “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas”

“Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Una definición más simple que se propone es la siguiente: Delito informático es el uso de cualquier sistema informático como medio o fin de un delito. De esta manera se abarcan todas las modalidades delictivas de acuerdo al marco legal de cada país; para esto es conveniente definir qué es un sistema informático.” (González, 2013)

Es necesario elaborar un concepto propio de delito informático haciendo una integración de los elementos comunes de la teoría del delito, (acción y omisión, típica, antijurídica, culpable y punible) haciendo referencia al uso de medios informáticos para su cometimiento y estableciendo la lesividad de esas conductas a bienes jurídicos protegidos, dicho concepto incluirá, lo delitos informáticos propiamente tales y los delitos comunes cometidos por medios informáticos.

[3] A la fecha de elaboración del presente instrumento, el Estado de El Salvador no es miembro del tratado contra la Ciberdelincuencia.

Delito informático: es toda acción típica, antijurídica, culpable y punible cometida mediante el uso de medios informáticos con la finalidad de manipular, alterar o suprimir información contenida en la web o cuando se empleen medios informáticos para la comisión de hechos delictivos en perjuicio del patrimonio, la libertad sexual, el sistema democrático y cualquier bien jurídico protegido.

5.3. Plataformas electrónicas utilizadas comúnmente para el comercio electrónico en El Salvador

Las redes sociales como mecanismo cibernético de interacción y de actividades comerciales.

Las redes sociales en la actualidad son un medio de comunicación y difusión de información al alcance de la gran mayoría de la población salvadoreña, pudiendo interactuar con personas en todo el mundo sin necesidad de conocerse. Ello permite acceder a otro tipo de productos o servicios que se publican o difunden en redes sociales.

Según la ley de delitos informáticos en su artículo 3 literal q) se define como redes sociales "La estructura o comunidad virtual que hace uso de medios tecnológicos y de la comunicación para acceder, establecer y mantener algún tipo de vínculo o relación, mediante el intercambio de información."

Las redes sociales más comunes en El Salvador son Facebook, Instagram, "X", antes denominada Twitter, Tick Tock, entre otras, también existen otras plataformas electrónicas que permiten la comunicación personal a través de mensajes de voz, texto o videos, inclusive por video llamadas, entre las más comunes se encuentran WhatsApp, Snapchat, Facebook Messenger, Telegram, entre otras.

El elemento esencial de dichas plataformas es la interacción humana como forma de entretenimiento y ocio, sin embargo, ese entretenimiento atrae la atención de la persona humana que a la vez se vuelve consumista del contenido distribuido por medio de las redes sociales, lo que genera las condiciones necesarias para ejercer el comercio electrónico.

Facebook, la mayor red social del mundo:

Según publicación en el portal electrónico denominado "el blog de Jose Facchin", Facebook es la red social más grande del mundo con más de tres mil millones de usuarios a nivel global

Según dicha publicación Facebook es una red social pensada para conectar personas, es decir, compartir información, noticias y contenidos audiovisuales con amigos y familiares. Propiedad de la empresa **Meta**, esta es la plataforma social más grande y popular de todas las existentes en la actualidad.

Es una red usada por personas de rangos de edad muy amplios, los cuales acostumbran a utilizarla a diario. Ésta, a pesar de ser tan popular, no está exenta de polémica. (FACCHIN, s.f.)

Facebook utiliza una combinación de técnicas para determinar tus intereses y mostrarte anuncios relevantes. Aquí te explico algunas de las principales:

1. **Datos de navegación**: Facebook rastrea tu actividad en la plataforma y en sitios web asociados. Esto incluye las páginas que visitas, los anuncios en los que haces clic, y las búsquedas que realizas[1].
2. **Interacciones en la plataforma**: Las publicaciones que te gustan, los comentarios que haces, y los grupos a los que te unes también ayudan a Facebook a entender tus intereses[1].
3. **Información de terceros**: Facebook puede recibir datos de otras empresas con las que colabora. Por ejemplo, si compras algo en un sitio web asociado, esa información puede ser utilizada para mostrarte anuncios relacionados[2].
4. **Encuestas y estudios de mercado**: Facebook también utiliza aplicaciones como Viewpoints para recopilar datos directamente de los usuarios a través de encuestas y estudios de mercado[2].

Estas técnicas permiten a Facebook crear un perfil detallado de tus intereses y comportamientos, lo que les ayuda a mostrarte anuncios que probablemente te interesen.

Instagram

Instagram es una red social muy popularizada entre jóvenes que **ofrece la posibilidad de compartir fotografías con otros usuarios** y poder recibir comentarios o "me gustas" (likes) de tus seguidores. Dentro de estas fotografías que podemos subir, podemos añadir **etiquetas o hashtags** para etiquetar según el tipo de fotografía o que se puede ver en ella, así será más fácil su clasificación a la hora de realizar búsquedas de una temática en concreto.

Creada inicialmente en exclusiva para iPhone, Instagram vio la luz en la App Store de Apple en octubre de 2010, y no fue **hasta abril de 2012 cuando salió la aplicación final para Android**, consiguiendo más de un millón de descargas en sus primeras 24 horas. Tanto fue el éxito que enseguida **Facebook se interesó por esta aplicación y red social que decidió comprarla**. En el año 2016, Instagram estrenaría su aplicación para Windows 10, aunque sin posibilidad para subir fotos. (GEEKNETIK, s.f.)

X (TWITER)

X (Twitter) es una red social de microblogging, que permite enviar mensajes de 280 caracteres (aún más, si tienes X Premium), que pueden ser vistos por otros usuarios y puedes seguir a otras cuentas de tu interés, además de conseguir seguidores que, a su vez, te sigan a ti.

Dichos mensajes son denominados «tweets» tuits y, aunque estos concretamente son públicos. También es posible iniciar conversaciones privadas, donde estos mensajes son denominados DM (Direct Messages ó «mensajes directos»). (FACCHIN, s.f.)

Tiktok

Tik Tok es una **red social a través de la que compartir vídeos de corta duración** con efectos, edición, música o filtros. Estos vídeos pueden durar entre 15 y 60 segundos.

Fue en 2018 cuando apareció por primera vez esta aplicación móvil. La empresa china ByteDance creó la famosa red social después de comprar lo que antes era Musical.Ly.

La aplicación cuenta con un algoritmo[4] que busca mostrarle al usuario aquello que le gusta. ¿Cómo sabe la plataforma qué tipo de contenido me gusta?
Pues muy sencillo: analiza qué vídeos ves hasta el final y con cuáles interaccionas, de esta forma **aprende qué te gusta y empieza a mostrarte contenido del mismo tipo.**

Aplicaciones de mensajería:

Las aplicaciones de mensajería son programas informáticos que permiten a los usuarios comunicarse entre sí mediante el envío y la recepción de mensajes de texto, voz, imágenes, vídeos y otros tipos de archivos. Estas aplicaciones funcionan de manera general mediante el uso de protocolos de Internet que establecen la conexión entre los dispositivos de los usuarios y los servidores de las empresas que ofrecen el servicio.

Los mensajes se almacenan temporal o permanentemente en los servidores y se transmiten a los destinatarios cuando estos se conectan a la red. Algunas aplicaciones de mensajería ofrecen también funciones adicionales como llamadas de voz o vídeo, grupos de chat, stickers, emojis, bots y otras herramientas interactivas. (DROIDERS, s.f.)

Las aplicaciones de mensajería sustituyeron los mensajes de texto de una forma más ágil, atractiva e interactiva, permitiendo una comunicación más fluida y más amena entre las personas.

Comunicación a través de correo electrónico:

El correo electrónico es una de las formas más antiguas de comunicación por medios informáticos y que a la fecha sigue vigente, como una forma de comunicación directa de persona a persona para compartir información.

El correo electrónico tal y como lo conocemos hoy en día tuvo su origen en los laboratorios de investigación de la década de 1960. Fue allí donde un grupo de científicos,

[4] Un **algoritmo** es un conjunto finito de operaciones simples que se define con precisión y se sigue de manera ordenada para resolver un problema específico. Estas operaciones deben ser **lógicas y ejecutables** por una computadora o máquina.**Fuente especificada no válida.**

comprometidos con la idea de crear una forma más rápida y eficiente de comunicación, dieron vida al primer sistema de envío de mensajes electrónicos.

El primer correo electrónico fue enviado en 1971 por Ray Tomlinson, un ingeniero informático legendario. El innovador sistema que desarrolló permitía enviar mensajes entre diferentes computadoras, lo que revolucionó la forma en que las personas se comunicaban. Y así, nació lo que hoy en día es una de las herramientas de comunicación más utilizadas en todo el mundo. (CURIOSAWEB, s.f.)

5.4. Comercio electrónico en El Salvador:

El diccionario de la Real Academia de la Lengua Española define el comercio como la "Compraventa o intercambio de bienes o servicios", (ESPAÑOLA, s.f.) Terminología que engloba en cuatro conceptos "compraventa", "intercambio", "bienes", "servicios" todas las actividades que comprenden el ejercicio del comercio en todas sus formas.

El Código de Comercio de El Salvador en su "LIBRO PRIMERO", denominado "LOS COMERCIANTES Y SUS AUXILIARES" no delimita el concepto de comerciante pero debe entenderse como comerciante: "la persona natural o jurídica que ejerce el comercio".

Según el código de comercio los comerciantes se clasifican en personas naturales "denominados comerciantes individuales" y personas jurídicas denominadas "comerciantes sociales".

En lo concerniente al comerciante individual, el código de comercio otorga capacidad para ejercer dicha actividad a las personas siguientes:

COMERCIANTE INDIVIDUAL Art. 7.-

Son capaces para ejercer el comercio:

I- Las personas naturales que, según el Código Civil son capaces para obligarse.
II- Los menores que teniendo dieciocho años cumplidos hayan sido habilitados de edad.
III- Los mayores de dieciocho años que obtengan autorización de sus representantes legales para comerciar, la cual deberá constar en escritura pública.

IV- Los mayores de dieciocho años que obtengan autorización judicial. Estas autorizaciones son irrevocables y deben ser inscritas en el Registro de Comercio.

Es necesario aclarar que el código de comercio vigente en El Salvador fue aprobado mediante decreto Legislativo número 671, del 8 de mayo de 1970, retomando la regulación del artículo 26 código civil que establecía la mayoría de edad a partir de los 21 años, artículo que ha sido reformado y en la actualidad la mayoría de edad se alcanza a partir de los 18 años.

En lo que respecta al comerciante social el código de comercio establece un concepto bastante en el artículo 17, el cual literalmente dice:

"Art. 17.- Son comerciantes sociales todas las sociedades independientemente de los fines que persiguen, sin perjuicio de lo preceptuado en el artículo 20.

Sociedad es el ente jurídico resultante de un contrato solemne, celebrado entre dos o más personas, que estipulan poner en común, bienes o industria, con la finalidad de repartir entre sí los beneficios que provengan de los negocios a que van a dedicarse.

Tales entidades gozan de personalidad jurídica, dentro de los límites que impone su finalidad, y se consideran independientes de los socios que las integran."

Del concepto de comerciante social brindado por el legislador se extraen las siguientes particularidades; **a)** conformado por dos o más personas naturales; b) patrimonio propio, los socios ponen bienes en común a favor del comerciante social**; c)** se constituye mediante contrato solemne celebrado entre los constituyentes; **d)** reparto de beneficios de los negocios que realice el comerciante social; **e)** personalidad jurídica propia; **f)** independencia de los socios que la integran.

5.5. Responsabilidad penal del comerciante individual:

Por los delitos cometidos en el ejercicio del comercio el código penal en el artículo 32 establece quienes son responsables penalmente y dice de la siguiente manera: "Incurren en responsabilidad penal por el delito cometido, los autores, los instigadores y los cómplices.

Los autores pueden ser directos o pueden ser mediatos.

En los delitos culposos cada uno responde por su propio hecho."

Es interesante como el código de comercio denomina capaces de ejercer el comercio a las personas mayores de 21 años[5], ya que, el ejercicio de una actividad lucrativa como el comercio es un derecho del ser humano, pero todo derecho también conlleva obligaciones y responsabilidades.

Francisco Muñoz Conde denomina "Culpabilidad" a la responsabilidad atribuida a una persona de ser acreedor a un reproche y una sanción por la comisión de un delito, catalogando la culpabilidad como una "capacidad de la persona" citando a ENGISH de la siguiente manera: " Como decía ENGISH, aunque el hombre poseyera esta capacidad de actuar de un modo distinto a como realmente lo hizo, sería imposible demostrar en el caso concreto si usó o no de esa capacidad, porque aunque se repitiera exactamente la misma situación en la que actuó, siempre habrá otros datos, nuevas circunstancias, etc., que la harían distinta. La capacidad de poder actuar de un modo diferente a como se actuó es, por consiguiente, indemostrable." (FRANCISCO MUÑOZ CONDE, 2004)

Definitivamente en materia de responsabilidad penal de la persona natural el código penal contiene una regulación basta y suficiente, sin embargo, cuando los delitos son cometidos por personas jurídicas la regulación es diferente.

5.6. Responsabilidad civil de las personas jurídicas según el Código de Comercio:

Las personas jurídicas o comerciantes sociales pueden dividirse en "SOCIEDADES DE RESPONSABILIDAD LIMITADA" y "SOCIEDADES DE RESPONSABILIDAD ILIMITADA"

Sobre las Sociedades de Responsabilidad Limitada e Ilimitada, el Doctor Roberto Lara Velado establece sobre las primeras los siguiente: "Habiendo nacido la figura como una consecuencia de la necesidad de limitar la responsabilidad de los socios, todos ellos no obstante la naturaleza personalista de la sociedad, responden limitadamente." En lo que respecta a las Responsabilidad Ilimitada en las Sociedades establece que " La responsabilidad

[5] 18 años en la actualidad

ilimitada de los socios es una garantía para los terceros, dentro de este tipo de sociedad. De tal manera, que la solidaridad y la responsabilidad ilimitada no pueden derogarse por pactos, frente a terceros, pero si entre los socios. (VELADO)

5.6.1 Responsabilidad limitada:

En el contexto empresarial, la responsabilidad limitada se refiere a la estructura legal de una entidad, como una sociedad de responsabilidad limitada (SRL) o una sociedad anónima (SA). Bajo este régimen, los propietarios o accionistas no son personalmente responsables por las deudas y obligaciones de la empresa más allá de su inversión inicial.

En otras palabras, si una empresa con responsabilidad limitada enfrenta problemas financieros o legales, los propietarios solo están expuestos a perder la cantidad de dinero que han invertido en la empresa y no sus activos personales. Esta característica brinda una protección adicional y un mayor nivel de seguridad para los propietarios de negocios.

5.6.2. Responsabilidad ilimitada:

Por otro lado, la responsabilidad ilimitada implica que los propietarios de una empresa son personalmente responsables de todas las deudas y obligaciones de la empresa, incluso más allá de su inversión inicial. Este tipo de responsabilidad suele ser aplicable a empresas individuales o sociedades en general.

En caso de dificultades financieras o legales, los propietarios con responsabilidad ilimitada pueden verse obligados a vender sus activos personales para cubrir las deudas de la empresa. Esto implica un mayor nivel de riesgo personal y una exposición significativa en caso de disputas legales o situaciones adversas. (LEGAL, s.f.)

La responsabilidad a la que se refiere el presente apartado es de carácter patrimonial y constituye una vinculación de los socios con la persona jurídica, sin que la misma implique la inobservancia de la independencia de la sociedad con los socios que la integran.

5.6.4. Responsabilidad civil de las personas jurídicas según el Código Penal.

El título VI del Código Penal, denominado "CONSECUENCIAS CIVILES DEL HECHO PUNIBLE", regula las diferentes formas de responsabilidad civil generadas por la comisión de hechos delictivos y no excluye de su regulación a las personas jurídicas, es así que el artículo 121, contempla la responsabilidad civil de las personas jurídicas como "responsabilidad civil subsidiarias especial", y la expone de la siguiente manera:

Responsabilidad civil subsidiaria especial Art. 121.-

La responsabilidad civil subsidiaria es especial, cuando el que responde por los daños y perjuicios provenientes del hecho punible cometido por el imputado, es una persona jurídica, o, en su caso, se trate del Estado o cualquiera de sus entes autónomos. En el primer caso, resultan obligados subsidiariamente:

1) Las personas jurídicas dueñas de empresas o establecimientos en que se cometió un hecho punible por parte de sus administradores, dependientes o cualquier trabajador a su servicio o cuando el hecho se suceda fuera de él, pero en razón de una actividad laboral;

2) Las personas jurídicas cuyos gerentes, administradores o personeros legales, resulten responsables de los hechos punibles; y,

3) Los que señalen las leyes especiales. En el segundo caso, resulta obligado subsidiariamente el Estado, por los daños y perjuicios derivados de los hechos punibles cometidos por sus funcionarios o empleados con motivo del desempeño de sus cargos; de igual manera responderán las instituciones públicas autónomas y las municipalidades cuando así expresamente lo ordene la ley."

Subsidiariedad y especialidad son dos características que se le atribuyen a la responsabilidad civil de las personas jurídicas, la primera hace referencia a que se trata de una responsabilidad de "ultima ratio", que procederá cuando los autores del delito no tengan la capacidad para reparar los daños económicos causados por la comisión de delitos y; especialidad hace referencia a que solo procederá en los casos previstos en la ley.

5.6.5 Responsabilidad penal del comerciante social "Personas Jurídicas"

Actualmente en El Salvador no existe un cuerpo normativo que establezca y regule la responsabilidad penal de las Personas Jurídicas, a pesar de que actualmente existe una propuesta de Ley de Responsabilidad de las Personas Jurídicas "LRPJ", que no ha tenido mayor avance en el congreso salvadoreño.

Sobre dicha propuesta el Consejo Directivo de la Superintendencia de Competencia ha emitido una opinión, mediante resolución de las nueve horas y catorce minutos del día treinta de enero de dos mil diecinueve, con referencia SC-003-S/ON/R-2019-Res.30/01/19 en la que en algunos de sus pasajes se lee: " 1. El 15 de enero de 2019, en las oficinas de la Superintendencia de Competencia, se recibió nota firmada por el licenciado Salvador Aníbal Osorio Rodríguez, Subsecretario para asuntos Legislativos y Jurídicos de la Presidencia de La República, por medio de la cual solicita opinión sobre (i) una propuesta de "Ley de Responsabilidad Penal de las Personas Jurídicas para la Comisión de Delitos" (LRPJ) y (ii) otra propuesta de reforma para adicionar el delito de "Soborno en el Sector Privado al Código Penal". (COMPETENCIA, 2019)

Como se dijo con anterioridad, no existe en la legislación salvadoreña cuerpo normativo alguno que establezca responsabilidad penal para las personas jurídicas, pero ello no implica que no se puedan perseguir penalmente las acciones punibles cometidas en el ejercicio del comercio.

5.7. El "actuar por otro", en la legislación salvadoreña

A pesar de no existir una legislación especial que regule la responsabilidad penal de las personas jurídicas, el código penal establece a quienes se les puede imputar la responsabilidad de los delitos cometidos por personas jurídicas o por medio de éstas. Dicha figura penal se denomina "ACTUAR POR OTRO" y tiene regulación en el artículo 38 del Código Penal que literalmente dice:

"ACTUAR POR OTRO

Art. 38.- EL QUE ACTUARE COMO DIRECTIVO, REPRESENTANTE LEGAL, O ADMINISTRADOR DE UNA PERSONA JURÍDICA, O EN NOMBRE O

REPRESENTACIÓN LEGAL O VOLUNTARIA DE OTRO, RESPONDERÁ PERSONALMENTE, AUNQUE NO CONCURRAN EN ÉL LAS CONDICIONES, CUALIDADES O RELACIONES QUE LA CORRESPONDIENTE FIGURA DEL DELITO REQUIERA PARA PODER SER SUJETO ACTIVO DEL MISMO, CUANDO TALES CIRCUNSTANCIAS SE DIEREN EN LA PERSONA EN CUYO NOMBRE O REPRESENTACIÓN OBRARE.

EN TODO CASO, LA PERSONA JURÍDICA INCURRIRÁ EN RESPONSABILIDAD CIVIL SUBSIDIARIA ESPECIAL. NO OBSTANTE, LO ANTERIOR, EN EL CASO DE LOS DELITOS DE COHECHO PROPIO, COHECHO IMPROPIO, COHECHO ACTIVO Y SOBORNO TRANSNACIONAL, LA PERSONA JURÍDICA SERÁ SOLIDARIAMENTE RESPONSABLE POR LOS DAÑOS CAUSADOS EN LOS TÉRMINOS ESTABLECIDOS EN EL ART. 118 DE ESTE CÓDIGO."

La responsabilidad penal por la comisión de hechos delictivos a través de personas jurídicas es atribuida directamente a las personas naturales que representan legalmente a dichas sociedades, lo que puede generar lugar a impunidades o persecuciones penales erradas. Sin embargo, no es el objeto de este apartado la discusión acerca de lo atinado o desatinado del criterio del legislador al respecto, sino hacer alusión a la regulación aplicable.

Al respecto de la figura del actuar por otro, la honorable sala de lo penal de la Corte Suprema de Justicia ha abordado la motivación del legislador para incorporar dicha figura en el artículo 38 del código penal, estableciendo lo siguiente:

"Esta Sala considera atinente, el mencionar que la razón que llevó a los legisladores a incorporar la figura jurídica del "Actuar por Otro" en el Código Penal, fue eliminar los espacios de impunidad en los que el actuante bajo el cobijo de la gestión ajena cometía o participaba en un hecho delictivo (Dependiendo del rol que le correspondería al suplido en el evento criminal), que no le era reprochable penalmente por haber cometido el acto en nombre de otro; de manera que en virtud de la cláusula en cita, el actuante responde personalmente por la acción u omisión típica que desplegó en el evento criminal, aunque no esté revestido de las condiciones, cualidades o relaciones del suplido, necesarias para tenerle

como sujeto activo del delito". ***Sentencia de Casación de las ocho horas con treinta y cinco minutos del día treinta y uno de octubre de dos mil dieciséis con referencia 22CAS2015*** (VLEX, s.f.)

Según el artículo 22 del Código de Comercio la creación de una persona jurídica debe realizarse a través de una escritura pública denominada "escritura de constitución" o "Pacto Social" y según el numeral IX- se debe establecer en el pacto social el "Régimen de administración de la sociedad, con expresión de los nombres, facultades y obligaciones de los organismos respectivos".

En el régimen de administración se deberá nombrar a una persona que ejerza la representación legal de la sociedad, comúnmente denominado "Representante Legal", siendo un concepto de carácter genérico para referirse a los mandatarios de las sociedades llámense "Administrador único, Director, Gerente, etc."

Ese mandato debe ser aceptado y convalidado por el representante legal ejerciendo actos de administración de la sociedad, los lineamientos de su actuación serán delimitados en el mismo pacto social, constituyendo un mandato imperativo de buena administración.

La persona jurídica no suele estar conformada por el organismo director o representante legal, sino por una pluralidad de personas en las que se ejerce una cadena de mando desde el representante legal, hasta los empleados de la misma.

Sobre: LA IMPUTACIÓN DE LA AUTORÍA EN EL MARCO DE ORGANIZACIONES DE CARÁCTER EMPRESARIAL, el maestro muñoz conde contempla un criterio más amplio que el del actuar por otro: "En el ámbito de estas organizaciones, como por ejemplo cualquier sociedad empresarial de cierta importancia, las actividades se realizan a través de un complejo organigrama, basado en la división de funciones en el plano horizontal y en la relación jerárquica en el plano vertical. Es, por ello, evidente que no puede situarse en el centro de gravedad de la responsabilidad por autoría solo o principalmente en el último eslabón de la cadena, es decir, la fase ejecutiva, dejando en la periferia o incluso en la impunidad conductas no ejecutivas, pero tan importantes o más que las propiamente ejecutivas. En este ámbito los <<centros de decisión>> son normalmente más importantes que los <<centros de ejecución>>.

El problema dogmático consiste en hallar el criterio material que permita atribuir a los que deciden la ejecución de un hecho delictivo la cualidad de autor, autor mediato o coautor, aunque no intervengan en su ejecución. Para ello solo deben tener en cuenta la estructura y modo de funcionamiento de las organizaciones en cuyo seno se comentan los delitos, sino también la propia naturaleza del delito en cuestión" (FRANCISCO MUÑOZ CONDE, 2004)

De manera que al integrar los conceptos legislativos y doctrinarios enunciados tenemos que los elementos esenciales de la figura del actuar por otro son los siguientes:

5.7.1 Existencia de un mandato de administración:

De conformidad con el artículo 22, numeral IX, del Código de Comercio en la escritura de constitución de la sociedad, se designa el ente administrador liderado por una figura unipersonal encargada de la administración, sin perjuicio de las decisiones colegiadas que se tomen.

En el caso de las sociedades nulas o irregulares, de conformidad con el artículo 348, del código de comercio establece que: .- Las sociedades a que se refieren los artículos anteriores, que se hubieren exteriorizado como tales frente a terceros, tienen personalidad jurídica únicamente en cuanto los perjudique, pero no en lo que pudiera beneficiarlos. Los socios, los administradores y cualesquiera otras personas que intervengan en su funcionamiento, responderán por las obligaciones de dichas sociedades frente a terceros, personal, solidaria e ilimitadamente, sin perjuicio de las responsabilidades penales en que hubieren incurrido. Las relaciones internas de estas sociedades se regirán por el pacto social respectivo, si lo hubiere; en su defecto, por las disposiciones generales contenidas en este Código, según la clase de sociedad de que se trate.

El Legislador determina responsabilidades en el actuar de las sociedades nulas e irregulares, extendiendo su regulación a la responsabilidad penal que pudiese generarse como consecuencia de las infracciones a los requisitos legales para la validez de las sociedades.

Es necesario aclarar, que al tratarse de sociedades nulas o irregulares existen más posibilidades de la comisión de hechos delictivos por no estar sujetas a los controles legales

correspondientes y al carecer de inscripción pueden generarse dificultades al momento de identificar a las personas con poder de decisión en las cadenas de mando de la sociedad.

5.7.2 Centros de decisión:

El Doctor Francisco Muñoz Conde, denomina centros de decisión a las personas o entes encargados de administrar la sociedad mercantil, quienes tienen rol de mando en los subordinados o ejecutores del delito, en consonancia con el artículo 38 del Código Penal, los representantes legales no solo delinquen por acción, sino que también por omisión, "realizando personalmente" "encomendando la realización" o "permitiendo que los subordinados o hagan"

5.7.3 Centros de ejecución:

En el organigrama de la empresa, los centros de ejecución están las personas que reciben las órdenes de los centros de decisión, los que habitualmente cometen los hechos delictivos, por mandato expreso de los centros de decisión o por omisión en su deber de prevención del delito de los mandatarios de la persona jurídica.

5.8. La figura jurídica del compliance como una forma de prevención del delito de empresa.

Si bien es cierto, el presente trabajo no se trata meramente de la Responsabilidad Penal de las Personas Jurídicas, no son temas aislados o contrapuestos a la presente investigación debido a que las estafas por medios informáticos pueden ser cometidas por personas naturales y también por personas naturales a través de la creación de personas jurídicas.

En ese orden de ideas es trascendental dejar clara la función del "compliance" en la prevención del delito de empresa y en la responsabilidad penal de las personas jurídicas.

5.8.1. Concepto de compliance:

Don Lenin González entrevistado para la revista Derecho y Negocios de El Salvador define la figura del "compliance" de la siguiente manera:

"En primer lugar por su mera traducción, significa cumplimiento. En segundo lugar, es importante acotar que, el compliance es una forma de autorregulación, pero no toda autorregulación es compliance.

En ese sentido, se entiende por compliance, el conjunto de mecanismos internos de una organización tendiente a asegurar el cumplimiento de la normativa que vincula-etica y legal-, en aras de prevenir y detectar los riesgos de incumplimiento a la referida normativa, y la reacción ante los mismos, que puedan generarse con la intervención propia de la persona jurídica.

Bajo esa precisión, no toda autorregulación podrá ser calificada como compliance para el caso, las que pretendan proteger a la empresa frente a delitos de terceros en la empresa, las de mejora de calidad, entre otras." (ISSUU, 2021)

Del concepto expuesto con anterioridad, se pueden identificar las características del compliance: **a) se trata de un cuerpo normativo interno:** definido como "autorregulación" se compone de un conjunto de normas ético legales creadas por las personas que tienen poder de decisión en la empresa, para ser aplicadas a la misma empresa; **b) finalidad preventiva:** el compliance es un mecanismo de control interno a las operaciones de la empresa para evitar la comisión de hechos delictivos; **c) finalidad reactiva:** el compliance también puede regular las respuestas o acciones que la empresa pueda tomar ante la comisión de hechos delictivos.

La figura del compliance no se encuentra regulada en la legislación salvadoreña, sin embargo su adopción pudiese ser beneficiosa en las actividades mercantiles de las empresas generando mayor estabilidad, certeza y sobre todo mecanismos de protección y prevención ante la comisión de delitos.

Por ejemplo, en El Salvador según la figura del "actuar por otro", el representante legal de la empresa tiene que responder de los delitos cometidos por o en dicha empresa, incluso puede ser acusado si un empleado comete el delito.

La adopción del compliance generaría un mecanismo procesal de defensa con el que se demuestra que las personas que tienen el poder de decisión en la empresa, crearon mecanismos de prevención de delitos porque su intención es ejercer el comercio, no la comisión de hechos delictivos y que el empleado o el tercero que ejecuta el delito, transgrede las normativas internas de forma dolosa para la consecución de un delito, lo que pudiese descartar responsabilidad penal o civil del representante legal y de la empresa.

5.9. Consideración especial a la extinción de dominio en El Salvador.

Por Decreto Legislativo número 534 de fecha siete de noviembre de dos mil trece, la Asamblea Legislativa de El Salvador aprobó la "LEY ESPECIAL DE EXTINCIÓN DE DOMINIO Y DE LA ADMINISTRACIÓN DE LOS BIENES DE ORIGEN O DESTINACIÓN ILÍCITA", como una consecuencia de carácter patrimonial a las personas naturales o jurídicas que obtengan beneficios económicos de actividades delictivas o que utilicen su patrimonio para delinquir.

Así lo establece en su artículo 2 que regula: "Art. 2.- Esta Ley se aplicará a los bienes de interés económico, de origen o destinación ilícitos ubicados dentro o fuera del territorio nacional, cuando su origen, incremento o destino se ubique dentro de los presupuestos contemplados en la misma, siempre que la acción de extinción de dominio sea iniciada en El Salvador."

Sobre la aplicación de la figura de la extinción de dominio a las personas jurídicas el legislador lo establece de forma expresa en la referida ley en el artículo 6, Literal c), que literalmente dice:

"Presupuestos de Procedencia de la Acción de Extinción de Dominio

Art. 6.- Son presupuestos de la procedencia de la acción de extinción de dominio, los siguientes:; c) CUANDO SE TRATE DE BIENES QUE CONSTITUYEN UN INCREMENTO PATRIMONIAL NO JUSTIFICADO DE TODA PERSONA NATURAL O JURÍDICA, QUE PROVENGAN DE ACTIVIDADES ILÍCITAS. ".

Manuel Adrián Merino Menjívar, en su tratado la Extinción de Dominio en El Salvador aclara que: la LEDAB define a la acción de extinción de dominio como una acción de carácter real y de contenido patrimonial, en cuanto se dirige contra bienes de origen o destinación ilícita. (MENJIVAR, 2022)

Por supuesto que la acción de extinción de dominio es una consecuencia jurídica de la comisión de delitos, pero de carácter civil, dirigida al patrimonio obtenido ilícitamente o utilizado para cometer ilícitos. Por lo tanto, no se puede definir la acción de extinción de

dominio, como una acción penal, tampoco ser considerada dentro del concepto de responsabilidad penal de las personas jurídicas.

5.9.1. La estafa informática en El Salvador

La estafa puede describirse, en general, como el hecho por medio del cual una persona toma, a raíz de un error provocado por la acción del agente, una disposición patrimonial perjudicial, que dicho agente pretende convertir en beneficio propio o de un tercero.
La secuencia causal en la estafa -como en toda defraudación por fraude- es la siguiente: el agente despliega una actividad engañosa que induce en error a una persona, quien, en virtud de ese error, realiza una prestación que resulta perjudicial para un patrimonio.
La conducta punible es, pues, la de *defraudar por medio de ardid o engaño.* (CREUS, 1998)
En el presente trabajo de investigación se hace un estudio pormenorizado de la figura penal denominada "Estafa Informática" regulada en la Ley Especial Contra Delitos Informáticos y Conexos.

En aras de una explicación más didáctica y sobre todo comprensible, se hará la segregación de los verbos rectores del tipo penal con su debido razonamiento.

Estafa informática Art. 10.-

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.

Se sancionará con prisión de cinco a ocho años, si las conductas descritas en el inciso anterior se cometieron bajo los siguientes presupuestos:

a) En perjuicio de propiedades del Estado;

b) Contra sistemas bancarios y entidades financieras; 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.

Verbos rectores:

Manipular o influenciar: una de las definiciones más acertadas que brinda la Real Academia de la Lengua acerca del vocablo manipular" es la de: "Intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la inf ormación, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulare s." (ESPAÑOLA, s.f.)

La manipulación o la influencia a que se refiere el artículo, aunque implique dificultades probatorias para establecerlo en juicio, admite las formas de autoría y participación. Para delimitar los conceptos de autoría y de participación Francisco Muñoz Conde acude al dominio del hecho, argumentando que: La distinción entre una y otra forma de intervención en el delito tiene que buscarse con un criterio objetivo-material. Este criterio objetivo-material es el del dominio del hecho. Según este criterio, es autor quien domina finalmente la realización del delito, es decir, quien decide en líneas generales el sí y el cómo de su realización. (FRANCISCO MUÑOZ CONDE, 2004)

Uso de datos falsos:

El tipo penal básico, también requiere uso indebido de información como "datos falsos" "alterando o modificando la programación de un sistema informático" o algún otro artificio que le permita al ciberdelincuente acceder al sistema.

Finalidad de la manipulación o influencia:

La finalidad de la manipulación del sistema informático es el "ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación".

Una vez se ha ingresado al sistema informático para acceder a través de un dispositivo electrónico, procede la intervención en los datos almacenados en el sistema web.

Ánimo de lucro:

El diccionario Panhispánico del Español Jurídico define el ánimo de lucro como: "Ganancia o provecho económico que se obtiene por la incorporación de la cosa al propio patrimonio. Exige algo más que el mero provecho.

El ánimo de lucro se agota con el animus rem sibi habendi, es decir, en el propósito de tener la cosa mueble para sí o, lo que es lo mismo, en la finalidad de desapoderar de la cosa al sujeto pasivo en forma definitiva, incorporándola, al menos transitoriamente, a su propio ámbito de dominio» (STS, 2.ª, 10-III-2000).

En el delito de estafa, el propósito de obtener una ganancia económica o de poseer o disponer de una cosa con valor económico como propia." (JURÍDICO, 2023)

Muchas leyes requieren taxativamente la obtención de un beneficio para el agente o para un tercero como elemento típico indispensable para la consumación de la estafa, lo cual no pasa con la nuestra: habiéndose producido la disposición patrimonial perjudicial, es indiferente que haya llegado o no a convertirse en beneficio para el autor o para un tercero. Pero está de acuerdo la doctrina en que el proponerse un beneficio ilegítimo como resultado de la acción estafadora es un requisito subjetivo de ella, ya que se trata de una exigencia propia de la noción de defraudación. Tiene que ser un beneficio ilegítimo: cuando la prestación de la víctima es debida por ella al agente o al tercero, no habrá estafa; quien utiliza un ardid para lograr que alguien le pague lo que le debe realmente o le devuelva lo que tiene que devolverle, no lo habrá estafado, ya que el patrimonio del sujeto pasivo del engaño no se verá *perjudicado* por quitarse de él lo que debía quitarse; no se tratará, por tanto, de una prestación no compensatoria que, como dijimos, es elemento imprescindible de la figura. (CREUS, 1998)

Agravantes:

El legislador ha cualificado las conductas descritas en el tipo penal en los casos que se exponen a continuación:

a) En perjuicio de propiedades del Estado;

b) Contra sistemas bancarios y entidades financieras; 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.

El fin de protección de bienes jurídicos de la norma penal a través de la pena es más extensivo en lo que se refiere a ataques cibernéticos en contra del Estado, por la pluriofensividad de las conductas prohibidas.

En el literal a) se trata de proteger los bienes que pertenecen al estado de aquellos ataques cibernéticos que generen afectación económica estatal, se entiende la calificación del tipo penal ya que una agresión cibernética compromete no solo la seguridad informática, sino también refleja un mayor grado de peligrosidad del delincuente.

En el caso del literal b) hay una finalidad de protección al sistema financiero, que suele ser donde más se generan las estafas informáticas, sin embargo, es necesario delimitar aquellos ataques directamente al sistema bancario o financiero de los ataques a los particulares a través del sistema financiero.

En los primeros se trata de vulnerar la seguridad informática de la banca y en el segundo supuesto sorprender la buena fe de los usuarios de la banca para que permitan el acceso a su información personal o bancaria.

Finalmente, el literal c), agrava la pena de quien teniendo a su cargo el uso, administración y protección de los sistemas informáticos estatales y que aprovecha su posición para defraudar al Estado.

5.9.2. La estafa electrónica y el incumplimiento de contrato:

El Derecho penal económico se caracteriza por la mixtura de ramas jurídicas que lo abastecen, por lo que se procederá a continuación a hacer un análisis escalonado de las normas jurídicas que podrían vulneradas en la comisión del delito de estafa electrónica en contraste con el incumplimiento de contrato, hasta llegar al derecho penal como ultima ratio, para poder establecer si se trata efectivamente de un delito penal o del mero incumplimiento de una obligación contractual.

El código civil salvadoreño a partir en el “LIBRO CUARTO”, “DE LAS OBLIGACIONES EN GENERAL Y DE LOS CONTRATOS” establece una regulación bastante completa en cuanto a la materia, definiendo el concepto de contrato a en el artículo 1309 de la manera siguiente: “contrato es una convención en virtud de la cual una o más personas se obligan para con otra u otras, o recíprocamente a dar, hacer o no hacer alguna cosa”

El artículo 1416 por su parte regula que: “Todo contrato legalmente celebrado, es obligatorio para los contratantes, y sólo cesan sus efectos entre las partes por el consentimiento mutuo de estas o por causas legales.

Otro concepto doctrinario de obligación lo desarrolla la maestra Alejandra Garcia Tellez, de la siguiente manera: “Es la necesidad jurídica que tiene una persona denominada obligado-deudor, de cumplir voluntariamente a favor de otra persona, denominada acreedor, que le puede exigir una prestación de carácter patrimonial (pecuniaria o moral). Este concepto, en su aspecto derecho de crédito o personal, presenta una estructura formada por los siguientes elementos:

a) Sujetos, que son: a. Obligado-deudor. b. Acreedor.

b) Relación jurídica; que los une, y

c) Objeto, que es la prestación que se debe.” (TELLEZ)

Las estafas pueden originarse de cualquier contrato que conlleve la obligación de dar, hacer o no hacer, ya que la criminalidad tiene diversas e ingeniosas formas de defraudar a las víctimas mediante ardid o engaño.

5.9.3. Mutación de das modalidades de estafas electrónicas en la Era Post Covid-19

2020 fue un año bastante inusual para todos nosotros. Hubo confusión e incertidumbre en todo el mundo debido a la pandemia y la sociedad se arrastra lentamente hacia la normalidad. Como la gente se vio obligada a permanecer en casa, Internet desempeñó un papel crucial para ayudarles a llevar a cabo sus actividades cotidianas. Ahora que Internet es el lugar al que acudir para satisfacer diversas necesidades, los estafadores en línea han visto crecer exponencialmente el número de víctimas potenciales.

Según nuestro informe Global State of Scams, cabe esperar un **aumento del 40%** de las estafas en línea para 2020. Varios países informan de que el fraude en línea se está convirtiendo en **el delito más denunciado**. Existen varios tipos diferentes de estafas en línea, ya que los estafadores siguen ideando formas innovadoras de defraudar a los consumidores. En este artículo, hemos enumerado las 10 principales estafas en línea que los internautas deben tener en cuenta. (SCAMADVISER, 2020)

Estafas de Phishing:

Las estafas de phishing se presentan en forma de llamadas telefónicas, correos electrónicos y mensajes de texto diseñados para hacerse pasar por una empresa legítima. Por ejemplo, puede recibir un correo electrónico de "PayPal" informando de que hay un problema con su cuenta que debe resolver inmediatamente, o puede recibir un mensaje de "Netflix" ofreciéndole un mes de suscripción gratuita si responde a una encuesta. El verdadero propósito de estos mensajes es robar su información personal y sus credenciales de acceso.

Las estafas de phishing son relativamente fáciles de evitar si estás atento. Compruebe si el mensaje procede de una dirección de correo electrónico oficial y si le redirige al sitio web real de la empresa. Evite hacer clic en los enlaces de mensajes y correos electrónicos, y sólo inicie sesión accediendo directamente al sitio web original. Según las estadísticas, el 96% de los ataques de phishing se realizan a través del correo electrónico. (SCAMADVISER, 2020)

La palabra phishing quiere decir suplantación de identidad, es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y asi apropiarse de la identidad de esas personas.

Los ciberdelincuentes envían correos electrónicos falsos como anzuelos para “pescar” contraseñas y datos personales valiosos. (ARGENTINA, 2024)

Estafas de Phishing en el año 2025 en El Salvador:

20 De Diciembre De 2024

Por Decreto Legislativo No. 185 de fecha 20 de diciembre de 2024, publicado en el Diario Oficial No. 244, Tomo 445 de fecha 20 de diciembre de 2024, se reformó la LEY DE

TRANSPORTE TERRESTRE TRÁNSITO Y SEGURIDAD VIAL, con la finalidad de incrementar el monto de las multas por infracciones de tránsito.

9 De Enero De 2025

En fecha 9 de enero de 2025 en el Salvador se implementó el sistema de "fotomultas" a través de dispositivos instalados en las carreteras capaces de detectar infracciones de tránsito según el portal web del periódico digital el cenit, dicho portal realizó la siguiente publicación:

El Viceministerio de Transporte (VMT) ha anunciado que a partir del jueves 9 de enero de 2025 implementarán un sistema de fotomultas en el bulevar Monseñor Romero, con el objetivo de reforzar el cumplimiento de la normativa de tránsito y mejorar la seguridad vial.

El bulevar Monseñor Romero es una vía de alta circulación que conecta diversos sectores de la capital salvadoreña. La implementación de las fotomultas busca reducir accidentes de tránsito causados por infracciones como el exceso de velocidad, el irrespeto a los semáforos y la invasión de carriles.

El VMT ha informado que las cámaras instaladas en puntos estratégicos del bulevar captarán imágenes de los vehículos que cometan infracciones, generando automáticamente una multa que será notificada al propietario del vehículo. (CENIT, 2025)

15 De Enero De 2025

El Viceministerio de Transporte de El Salvador emite una alerta sobre estafas con fotomultas falsas, el cual fue publicado por el portal de noticias Que pasa SV.

El Viceministerio de Transporte (VMT) ha emitido una alerta sobre una nueva modalidad de estafa que afecta a conductores en El Salvador. La estafa consiste en el envío de mensajes de texto con falsas notificaciones de fotomultas, dirigidas a los usuarios con el fin de obtener pagos fraudulentos.

Según informó el VMT, las notificaciones oficiales por infracciones de tránsito incluyen detalles específicos como la fecha en que se cometió la infracción, el número de referencia o infracción, el código, el concepto y el monto de la multa. La institución enfatizó que los conductores deben evitar ingresar a enlaces sospechosos y utilizar exclusivamente el sitio web oficial sertracen.com.sv/consultamultas para consultar y pagar esquelas.

El VMT también aclaró que el pasado 14 de enero realizaron pruebas de sistema mediante el envío de correos electrónicos y mensajes de texto simulando notificaciones de multas. Sin embargo, destacaron que estas pruebas no requieren ningún pago por parte de los usuarios. (SV, 2025)

Puede verse la facilidad y la rapidez con que la criminalidad informática genera nuevas formas de estafa electrónica, a través del phishing para lucrarse económicamente.

Estafas piramidales:

Muchas de las oportunidades de inversión disponibles en Internet son esquemas fraudulentos. Mientras que las inversiones a través de medios legítimos pueden generar entre un 1% y un 15% al año, los estafadores ofrecen el mismo tipo de rendimientos diaria o semanalmente. Utilizan identidades falsas y se dirigen directamente a la gente a través de las redes sociales o de anuncios en Internet. Se dirigen a personas que no son inversores activos y que, por tanto, no son lo bastante inteligentes para reconocer lo absurdo de las promesas del estafador. (SCAMADVISER, 2020)

¿Qué es una estafa piramidal?

Una **estafa piramidal** es un esquema en el que los ingresos de los participantes no provienen de la venta real de bienes o servicios, sino de las aportaciones de nuevos participantes. Es insostenible y colapsa cuando no hay suficientes nuevos miembros para sostener el sistema.

Estafas piramidales por medios informáticos:

Estas estafas se valen de **internet, redes sociales, correos electrónicos, aplicaciones móviles, criptomonedas y sitios web** para promocionar sus esquemas. Algunas características comunes:

- Promesas de **altos retornos** con poca inversión.
- Requieren **invitar a más personas** para generar ganancias.
- Uso de **lenguaje motivacional o pseudofinanciero** ("ingresos pasivos", "libertad financiera", etc.).
- Poca o nula transparencia sobre el producto o servicio.
- Sitios web con **estructura opaca o falsa**, sin datos legales claros.

Ejemplos comunes en internet

1. **Criptomonedas falsas o tokens sin respaldo real** (ej. Bitconnect, Forsage).
2. **Cursos o membresías** donde se gana dinero solo reclutando más personas.
3. **Apps o plataformas de inversión** que requieren referidos para obtener beneficios.
4. **Esquemas "gifting"** disfrazados de redes solidarias.

¿Cómo identificar una estafa piramidal online?

- Exigen **inversiones iniciales obligatorias**.
- No existe un **producto o servicio claro**.
- Los ingresos dependen del número de referidos.
- Sitios sin **términos legales visibles ni información de contacto verificable**.
- Te piden que **aportes más dinero** o "subas de nivel" para ganar más.

Legislación y consecuencias legales

En muchos países, las estafas piramidales están **prohibidas por ley**, incluso cuando se hacen por medios digitales. En el caso de **España o países de América Latina**, se pueden aplicar leyes como:

- **Delito de estafa** (Código Penal).

- **Delitos informáticos** (cuando se usa internet o software para defraudar).
- **Ley de Protección al Consumidor** (por publicidad engañosa o falta de transparencia).
- En el caso de criptoactivos: **regulación financiera y de valores**, si aplica.

Tipos de estafas piramidales:

- **Pirámides abiertas.** En ellas quienes intervienen conocen la estructura. Hay quién considera que, por tanto, no sería una estafa. Aun así funcionan porque muchos no entienden el concepto de saturación del mercado o creen que están tan arriba como sea necesario.

- **Pirámides cerradas.** En este caso una persona o una institución serían los dueños de dicha pirámide. Ellos prometen ganancias a aquellos que entran nuevos, pero en realidad, les están pagando con los beneficios de otros. Un caso muy conocido es el esquema Ponzi que utiliza los beneficios de unos inversores para pagar intereses a otros nuevos. (ECONOMIPEDIA.COM, s.f.)

5.9.4. Estafas románticas o "Romantic Scam"

La cuarentena domiciliar obligatoria a nivel nacional e internacional generó un encierro prolongado de la población, lo que tuvo un impacto emocional y psicológico en los seres humanos, sin embargo, el acceso a internet y redes sociales fue una forma de comunicación interpersonal sin exponerse a un posible contagio del covid-19.

Esa interacción electrónica, no solo género relaciones comerciales entre desconocidos detrás de sus dispositivos electrónicos, sino también relaciones del tipo amoroso entre desconocidos o "conocidos a través de internet" lo que permitió que muchos se aprovechan de la vulnerabilidad emocional de las víctimas para sacar provecho económico.

Definición de estafa amorosa:

Una estafa amorosa se define como un esquema fraudulento donde un estafador crea una falsa identidad romántica en plataformas de citas o redes sociales para atraer a la víctima. El objetivo principal es ganar la confianza de la persona afectada, creando una relación

emocional que facilite el eventual engaño financiero. Este tipo de estafas puede tener consecuencias devastadoras tanto emocionales como financieras. (LAW&TRENDS, s.f.)

La **estafa electrónica mediante relaciones amorosas por redes sociales** se conoce comúnmente como **"estafa romántica" o "romance scam"**, y es uno de los fraudes digitales más frecuentes y emocionalmente devastadores. Los estafadores se aprovechan de la vulnerabilidad emocional de sus víctimas para obtener **dinero, datos personales o acceso a cuentas**.

¿En qué consiste?

El estafador crea una **identidad falsa en redes sociales, aplicaciones de citas o incluso plataformas como Facebook o Instagram**, y establece una relación afectiva con la víctima. Con el tiempo, construyen confianza y luego inventan una excusa para pedir **dinero, regalos o favores financieros**.

Etapas comunes de la estafa romántica

1. **Captación**: Usan perfiles falsos con fotos atractivas (a menudo robadas de modelos o militares).
2. **Conexión emocional rápida**: Declaran amor o interés profundo en poco tiempo.
3. **Manipulación emocional**: Se muestran atentos, cariñosos, vulnerables, y crean una sensación de urgencia emocional.
4. **Petición de dinero**: Alegan problemas de salud, viajes, accidentes, deudas o emergencias (médicas, familiares, legales).
5. **Persistencia y amenazas**: Si la víctima se niega, pueden manipular con culpa, o incluso extorsionar con imágenes íntimas.

Señales de alerta

- Te escriben **con mucha intensidad** al poco tiempo de conocerte.
- Declaran amor **muy rápido** o sin haberte visto en persona.
- Dicen estar en el **extranjero** (militar, ingeniero, médico en zona de guerra, etc.).

- Siempre hay una **excusa para no encontrarse en persona o hacer videollamadas reales**.
- Te piden **dinero por transferencias, criptomonedas, tarjetas regalo o billeteras electrónicas**.
- Usan un lenguaje muy formal o con errores típicos de traducción automática.

Modalidades comunes

- **Estafas con criptomonedas**: Primero fingen ayudarte a invertir y luego desaparecen.
- **Sextorsión**: Piden fotos íntimas y luego amenazan con difundirlas si no pagas.
- **Falsos matrimonios o visas**: Simulan querer casarse o viajar, y piden dinero para trámites.
- **Estafas con envío de paquetes**: Dicen enviarte algo valioso y luego piden que pagues aduanas falsas.

Implicaciones legales

Este tipo de estafa puede ser tipificado como:

- **Estafa informática o electrónica**.
- **Suplantación de identidad**.
- **Extorsión o chantaje** (en casos de sextorsión).
- En algunos países, se considera **violencia digital o violencia de género**, si hay abuso emocional reiterado.

5.9.5. Estafas electrónicas mediante compras en línea post Covid-19

Después de la pandemia de COVID-19, **las compras en línea crecieron exponencialmente**, lo que también dio lugar a un aumento significativo de los **fraudes en compras online**. A continuación te explico los tipos más comunes de fraudes en este ámbito, cómo reconocerlos y cómo protegerte.

5.9.6. Fraudes en compras online post-Covid-19

Tiendas falsas

- Sitios web o perfiles en redes sociales que **simulan ser tiendas legítimas**, pero no envían nada.
- Ofrecen **productos populares a precios excesivamente bajos**.
- Suelen desaparecer en poco tiempo y cambiar de nombre.

Ejemplo: Un sitio que vende zapatillas de marca a mitad de precio, pero nunca hace entregas.

Phishing en sitios de compras

- Imitan páginas como Amazon, Mercado Libre, AliExpress, etc.
- Envían **correos falsos** con ofertas, estados de pedidos o problemas con el pago.
- Al hacer clic, el usuario ingresa sus datos en un sitio falso y **roban sus credenciales o tarjetas**.

Estafas con envío

- Te dicen que tu pedido está retenido en aduanas, que hay un cargo adicional, o que debes confirmar información personal.
- En realidad, **no hay ningún pedido** y buscan robar datos o dinero.

También ocurre con **mensajes SMS falsos** de supuestas empresas de mensajería.

Productos diferentes o defectuosos

- Compras un artículo (ropa, tecnología, etc.) y recibes **algo completamente distinto, de mala calidad o falsificado**.
- Muchas veces vienen de sitios poco conocidos o de publicidad en redes.

Robo de datos bancarios

- Sitios no seguros (sin cifrado SSL o "https://") que almacenan o roban tu información de tarjeta.
- A veces usan pasarelas de pago falsas o piden pagos fuera de la plataforma (por transferencia directa, Bizum, etc.).

Anuncios engañosos en redes sociales

- Publicidades en Facebook, Instagram, TikTok o YouTube que llevan a tiendas fantasma.
- Imágenes y videos falsos para mostrar productos que no existen o no se parecen en nada a la realidad.

Ofertas irresistibles / ventas flash

- Promociones de tiempo limitado con **descuentos extremos (70%-90%)**.
- Usan el miedo a "perder la oferta" para que compres rápido sin verificar.

Estafas en marketplaces entre particulares

- Personas que venden por Facebook Marketplace, OLX o similares, y desaparecen después de recibir un pago.
- Productos que nunca llegan o que no son los prometidos.

Plataformas más utilizadas para estafas mediante compras online:

Google: Aunque no es una plataforma de compra y venta, Google suele ser el punto de partida para buscar precios, comparar y ver quiénes ofrecen el producto o servicio deseado. Sin embargo, no todo lo que aparece en los resultados es legítimo: pueden incluir sitios falsos, muchas veces mediante anuncios que aparecen en los primeros lugares.

Plataformas de comercio electrónico: En sitios como Mercado Libre, Amazon, Temu, AliExpress o eBay, uno de los riesgos que se comparten son los correos de phishing, en los cuales los cibercriminales intentan hacerse pasar por ellas, con el objetivo de que las víctimas

entreguen sus datos personales e información bancaria. Los motivos o señuelos pueden ser variados: desde un problema de seguridad o movimiento sospechoso en la cuenta, hasta un regalo, un sorteo o una oferta muy difícil de rechazar.

Tiendas ecommerce independientes: Muchos usuarios eligen comprar a emprendedores o pequeños comercios que venden desde su propia tienda online utilizando alguna herramienta para sumar un carrito de compras y la posibilidad de realizar pagos. En estos casos, el mayor peligro es que una tienda, aún con buena intención, haya sido comprometida sin saberlo.

Redes sociales: Una de las prácticas más comunes es la creación de perfiles falsos con nombres muy similares a los de cuentas verificadas. Hay casos de cuentas clonadas de entidades bancarias, personas particulares y marcas populares, donde hasta utilizan el logo oficial. A su vez, una de las herramientas más utilizadas por el cibercrimen es el scrapping que permite monitorear los comentarios y otra actividad de un perfil oficial y real, para luego ponerse en contacto con personas que dejan comentarios, por ejemplo solicitando ayuda porque hicieron un pedido. El objetivo de este engaño es obtener información o algún provecho económico.

Google: Aunque no es una plataforma de compra y venta, Google suele ser el punto de partida para buscar precios, comparar y ver quiénes ofrecen el producto o servicio deseado.Sin embargo, no todo lo que aparece en los resultados es legítimo: pueden incluir sitios falsos, muchas veces mediante anuncios que aparecen en los primeros lugares.

Plataformas de comercio electrónico: En sitios como Mercado Libre, Amazon, Temu, AliExpress o eBay, uno de los riesgos que se comparten son los correos de phishing, en los cuales los cibercriminales intentan hacerse pasar por ellas, con el objetivo de que las víctimas entreguen sus datos personales e información bancaria. Los motivos o señuelos pueden ser variados: desde un problema de seguridad o movimiento sospechoso en la cuenta, hasta un regalo, un sorteo o una oferta muy difícil de rechazar.

Otro engaño muy común es aquel en el que se invita a la víctima a seguir la conversación por fuera de la plataforma (ya sea por tema de pagos o de envíos). Como señuelo, se suelen

ofrecer artículos de gran valor y alta demanda (como celulares, computadoras) por precios muy bajos, y sugerir hacer el envío de manera particular, con un precio más costoso de lo normal. El resultado es que el ciberatacante se queda con el dinero del envío y el supuesto producto nunca llega al comprador.

Otras tiendas en línea

Tiendas ecommerce independientes: Muchos usuarios eligen comprar a emprendedores o pequeños comercios que venden desde su propia tienda online utilizando alguna herramienta para sumar un carrito de compras y la posibilidad de realizar pagos. En estos casos, el mayor peligro es que una tienda, aún con buena intención, haya sido comprometida sin saberlo.

Redes sociales: Una de las prácticas más comunes es la creación de perfiles falsos con nombres muy similares a los de cuentas verificadas. Hay casos de cuentas clonadas de entidades bancarias, personas particulares y marcas populares, donde hasta utilizan el logo oficial. A su vez, una de las herramientas más utilizadas por el cibercrimen es el scrapping que permite monitorear los comentarios y otra actividad de un perfil oficial y real, para luego ponerse en contacto con personas que dejan comentarios, por ejemplo solicitando ayuda porque hicieron un pedido. El objetivo de este engaño es obtener información o algún provecho económico.

Los anuncios también son una funcionalidad especialmente aprovechada para captar la atención de los usuarios, y mediante ellos se puede suplantar la identidad y ofrecer promociones atractivas, con el fin de obtener información personal y financiera.

Facebook marketplace: Si bien tener acceso a los perfiles de los vendedores da una sensación de seguridad, la misma a menudo es falsa: ya que es común escuchar de estafas y engaños que circulan en esta plataforma. Una de las estafas más comunes involucra productos defectuosos o que no existen. Puede pasar que el vendedor muestra un producto impecable en fotos, pero al recibirlo está dañado o no existe. Por eso siempre es importante verificar las reseñas y, en la medida de lo posible, probar las funcionalidades. (E&N, 2025)

5.9.7. Fraudes con inteligencia artificial

Los **deepfakes y fraudes con inteligencia artificial (IA)** se han convertido en una amenaza emergente y muy peligrosa en el mundo digital post-COVID-19. Aprovechan el avance de tecnologías de IA para **suplantar identidades, manipular imágenes, videos o voces, y cometer fraudes altamente convincentes**.

La inteligencia artificial está sirviendo para hacer cosas extremadamente positivas que antes hubiesen sido impensables, especialmente desde el punto de vista del procesamiento de datos a mayor escala.

Sin embargo, como se suele decir en España: "Hecha la ley, hecha la trampa".

Los ciberdelincuentes también han empezado a utilizar la tecnología para cometer sus fechorías. Aquí puedes ver cómo puedes defenderte de los peores usos de la IA (ARMERO, 2024)

¿Qué son los deepfakes?

Los **deepfakes** son contenidos manipulados por inteligencia artificial (especialmente modelos de aprendizaje profundo) que pueden:

- Cambiar el rostro o la voz de una persona en un video.
- Imitar la manera de hablar, expresarse o moverse.
- Hacer que alguien parezca decir o hacer algo que **nunca dijo o hizo**.

¿Qué tipos de fraudes se cometen con deepfakes o IA?

Suplantación de identidad (personal o empresarial)

- Usan la voz o imagen de un jefe o directivo para ordenar **transferencias de dinero** urgentes.
- Envían audios o videos falsos a empleados, proveedores o clientes.
- Pueden generar **correos o videollamadas falsas** que parecen legítimas.

Ejemplo real: Un empleado de una empresa financiera transfirió más de 35 millones de dólares tras recibir una videollamada falsa generada por IA.

Fraudes románticos con videos falsos

- Estafadores usan deepfakes para **crear perfiles falsos más creíbles** en apps de citas o redes sociales.
- Envían vídeos manipulados para generar confianza y luego piden dinero.

Fake news y manipulación política

- Videos falsos de líderes políticos diciendo cosas polémicas.
- Difunden información falsa durante elecciones o protestas, con fines de **desinformación o propaganda**.

Extorsión y sextorsión

- Suplantan a la víctima usando su rostro o voz en contenido sexual falso.
- Amenazan con difundir el material si no pagan una suma o entregan más datos.

Fraudes con clonación de voz

- Llamadas automatizadas que imitan a familiares para pedir dinero o ayuda.
- Estafadores usan audios breves de redes sociales para crear **clones de voz** altamente realistas.

Inversiones falsas con influencers o figuras públicas

- Videos falsos de celebridades recomendando criptomonedas, productos financieros o negocios inexistentes.
- Circulan especialmente en TikTok, Instagram y YouTube Shorts.

¿Cómo reconocer un deepfake o fraude con IA?

Signos de alerta:

- Movimientos faciales extraños, poco naturales o con desincronización entre voz y labios.
- Iluminación inconsistente en el rostro o parpadeo anormal.
- Pedidos urgentes de dinero, información o acciones bajo presión emocional.
- Contacto inesperado por videollamada o audio con personas de autoridad.

5.9.8. Estafas electrónicas mediante aplicaciones de mensajería "WhatsApp"

Después del COVID-19, el uso de **WhatsApp** se intensificó tanto para comunicación personal como laboral, lo que lo convirtió en un **canal privilegiado para estafadores digitales**. A continuación, te presento un resumen completo de las **estafas por WhatsApp más comunes post-pandemia**, cómo operan y cómo protegerte.

Suplantación de identidad de familiares o amigos

- El estafador se hace pasar por un ser querido usando un número nuevo.
- Envía mensajes como: *"Hola, cambié de número. ¿Me puedes hacer un favor?"*
- Luego pide dinero urgente por una supuesta emergencia.

Muy común con padres, hijos o abuelos que no verifican la identidad.

En El Salvador ha sido muy común este tipo de estafas, en donde los delincuentes se hacen pasar por un familiar en una situación de emergencia que requiere asistencia económica inmediata.

Estafa del "falso premio" o "bono gubernamental"

- Mensajes que dicen: *"Has ganado un premio", "Te corresponde un subsidio por COVID", o "El gobierno está entregando ayudas".*
- Incluyen un **enlace fraudulento** que roba datos personales o instala malware.

Estafa de verificación de cuenta (código de 6 dígitos)

- El estafador intenta iniciar sesión en tu WhatsApp y tú **recibes un SMS con un código de verificación**.
- Luego, te escribe haciéndose pasar por un conocido y te dice: *"Por error te llegó un código, ¿me lo puedes pasar?"*
- Si lo haces, **pierdes el acceso a tu cuenta**.

Estafa del "jefe falso"

- Usan un número desconocido con la foto y nombre de un superior del trabajo.
- Piden hacer una compra urgente, transferir dinero o compartir información confidencial.

Estafas en Ventas o Marketplace

- Estafadores se hacen pasar por compradores o vendedores.
- Envían comprobantes de pago falsos o piden anticipos.
- A veces usan métodos de pago no seguros (Bizum, transferencias directas, criptomonedas).

Estafas de Inversión

- Prometen grandes ganancias en poco tiempo invirtiendo en criptomonedas, forex o apuestas.
- Muestran capturas falsas de supuestos beneficios.
- Después de invertir, **te bloquean**.

Estafas con Amenazas Legales

- Recibes un mensaje diciendo que tienes una deuda, una denuncia o que la policía te busca.
- Piden que pagues para "detener el proceso" o para asesoría legal.

Falso mensaje de paquetería o encomienda

- Simulan ser DHL, FedEx, Correos, etc.
- Dicen que hay un paquete retenido y piden que **descargues un archivo o entres a un enlace** para liberarlo.

Señales de advertencia

- Número nuevo con excusas para no enviar audios ni hacer videollamadas.
- Mensajes con faltas de ortografía o estilo muy genérico.
- Enlaces sospechosos (bit.ly, enlaces acortados o dominios extraños).
- Solicitudes urgentes de dinero o datos personales.

Estafas más comunes mediante Whatsapp según el portal web HikiHow

Estafa del oro en WhatsApp. En esta estafa, recibirás un mensaje diciéndote que eres apto para una versión exclusiva de WhatsApp llamada "WhatsApp Gold". Se te pedirá que hagas clic en un enlace para descargar o actualizar la aplicación

Suplantación de un ser querido. Esta estafa es sumamente común en WhatsApp y otras aplicaciones de mensajería. El estafador finge ser un ser querido en necesidad, y te pedirá dinero o ayuda. Por ejemplo, el mensaje podría decir "Hola, mamá, soy yo. Tengo un número nuevo. Puedes eliminar el antiguo".

Tarjeta de regalo falsa o encuesta. Para esta estafa, los estafadores envían un enlace afirmando que has ganado una tarjeta de regalo o un premio gratis. La mayoría de las veces, no tendrás ninguna afiliación con la empresa con la que ganas algo.

Estafas con ofertas de trabajo. En esta estafa, los estafadores te seducen con una oferta de trabajo demasiado buena para ser verdad afirmando ser reclutadores de una empresa. Te prometerá salarios grandes por un trabajo pequeño y te preguntarán tu información personal o que pulses en un enlace para saber más.

Fraudes con códigos de verificación. En estas estafas, los estafadores solicitan un código de verificación enviado a tu teléfono. Podrían convencerte de que son un familiar o

amigo que utilizó por accidente tu número telefónico. Si proporcionas el código, podrán acceder a tu cuenta de WhatsApp.

Estafa del número equivocado. Esta estafa apela a tu bondad. Los estafadores inician una conversación por mensaje de texto preguntándote si tienen el número correcto afirmando que tienen un amigo en común o una asociación comercial. Luego, seguirán la conversación para familiarizarse contigo en un intento por obtener tu información personal.

Estafa de criptomonedas en WhatsApp. En esta estafa, los estafadores envían un mensaje afirmando ser de una empresa de criptomonedas. Ofrecerán rendimientos altos de la inversión o prometen ayudarte a empezar.

Fraudes de lotería y sorteos. Estas estafas afirman que has ganado un gran premio o la lotería. El estafador enviará un mensaje pidiéndote que hagas clic en un enlace para "reclamar" tu premio.

Estafas de romance. Por lo general, estas estafas empiezan en las aplicaciones de citas (como Tinder) y pasan a WhatsApp una vez que se hace *match*. Estos estafadores te llenarán de halagos o cumplidos hasta tener tu confianza. Luego, inventan situaciones de emergencia en las que necesiten que les envíes dinero para ayudarte.

Estafas de caridad. En estos tipos de estafas, los estafadores fingirán formar parte de una organización o institución benéfica. Te pedirán tu donación a una causa específica y te otorgarán un enlace para que puedas hacer una donación. Este enlace dirigirá los fondos a su cuenta personal, no a la de una organización benéfica legítima.

Suplantación del soporte técnico de WhatsApp. En esta estafa, los estafadores se harán pasar por representantes de WhatsApp. Se comunican con los usuarios indicando que tienen problemas con sus cuentas. Solicitarán información personal en un intento de "arreglar" la cuenta. Mientras tanto, les roban su información.

Alertas bancarias falsas. Los estafadores fingirán ser un mensaje automático de tu banco diciendo que alguien está intentando acceder a tu cuenta o que ha habido alguna actividad

fraudulenta en ella. Solicitarán tu información personal para solucionar el problema o te pedirán que hagas clic en un enlace para obtener más información.

Truco del desvío de llamada. En esta estafa, los estafadores intentan convencerte de que llames a un número específico. Al hacerlo, les das acceso a tu cuenta de WhatsApp. Esta estafa puede realizarse por teléfono o mensajería. (WIKIHOW, s.f.)

5.9.9. Fraudes financieros con criptomonedas.

Los **fraudes financieros con criptomonedas** han aumentado drásticamente en los últimos años, especialmente tras el auge post-pandemia de estas tecnologías. Muchos estafadores aprovechan la falta de regulación, el anonimato y la novedad del mundo cripto para engañar a inversores, ahorradores y personas sin experiencia.

La Comisión Federal de Comercio aclara lo que hay que saber sobre las criptomonedas y las estafas.

¿Qué es una criptomoneda?

La criptomoneda, también llamada moneda virtual, es un tipo de moneda digital que solo existe electrónicamente. Generalmente, para comprar una criptomoneda usted usa su teléfono, computadora o un cajero ATM de criptomonedas. Las criptomonedas más conocidas son Bitcoin y Ether, pero hay varias marcas diferentes, y continuamente se crean nuevas criptomonedas.

¿Cómo utiliza las criptomonedas la gente?

Las personas usan las criptomonedas por muchas razones, para hacer pagos rápidos, para evitar los cargos de transacción que cobran los bancos tradicionales o porque ofrecen algo de anonimato. Otras personas podrían adquirir y conservar criptomonedas como una inversión, con la esperanza de que aumente su valor.

¿Cómo se pueden obtener las criptomonedas?

Usted puede comprar criptomonedas a través de un agente de cambio, un sitio web o un cajero ATM de criptomonedas. Alguna gente puede adquirir criptomonedas a través de un proceso complejo llamado "minería" o "mining" para el cual se necesita un equipo de computación avanzado para resolver problemas matemáticos muy complicados.

¿Dónde y cómo se almacenan las criptomonedas?

Las criptomonedas se almacenan en un monedero o cartera digital, ya sea en línea, en su computadora o en otro soporte físico externo. Una cartera o monedero digital tienen un domicilio, que habitualmente, es una larga cadena de números y letras. Si sucede algo con su cartera o sus fondos en criptomonedas, por ejemplo, si la plataforma de cambio en línea que usa deja de operar, si usted le envía criptomonedas a la persona equivocada, pierde la contraseña de su cartera digital, le roban o hay algún problema con su cartera digital, es probable que descubra que no hay nadie disponible para ayudarlo a recuperar sus fondos.

¿Cuáles son las diferencias entre la criptomoneda y el dólar estadounidense?

Como las criptomonedas solo existen en línea, hay diferencias importantes entre las criptomonedas y las monedas tradicionales, como el dólar estadounidense.

- **Las cuentas de criptomonedas no están respaldadas por un gobierno.** Las criptomonedas que se mantienen en cuentas **no** están aseguradas por un gobierno como sí lo están los dólares estadounidenses depositados en una cuenta bancaria asegurada por la FDIC. Si sucede algo con su cuenta o sus fondos de criptomonedas, por ejemplo, la compañía que provee el servicio de almacenamiento de su cartera virtual deja de operar o sufre un ataque informático, el gobierno no tiene ninguna obligación de intervenir para ayudarlo a recuperar su dinero.
- **El valor de una criptomoneda cambia constantemente.** El valor de una criptomoneda puede cambiar rápidamente, incluso cada hora. Y el monto de esa fluctuación puede ser considerable. Su valor depende de muchos factores, incluyendo la oferta y la demanda. Las criptomonedas tienden a ser más volátiles que las inversiones tradicionales, como los bonos y acciones. Una inversión que hoy vale

miles de dólares mañana podría valer solo unos cientos de dólares. Y si el valor baja, no hay garantía de que vuelva a subir.

Estafas de inversiones

En las estafas de inversiones a menudo le prometen que puede "ganar mucho dinero" con "riesgo cero", y estas estafas suelen comenzar en los medios sociales o en aplicaciones o sitios de citas. Por supuesto que estas estafas también comienzan con un mensaje de texto, email o llamada. Y en las estafas de inversiones, la criptomoneda cumple un rol central de dos maneras: puede ser tanto para una inversión como para pagar.

A continuación, se enumeran algunas de las estafas de inversiones comunes y cómo detectarlas.

- **Un supuesto "gerente de inversiones" se comunica con usted inesperadamente.** Le promete multiplicar su dinero, pero únicamente si usted compra criptomonedas y se las transfiere a su cuenta en línea. El sitio web de inversiones al que lo dirigen parece real, pero es realmente falso, como sus promesas. Si inicia sesión en su "cuenta de inversión", no podrá retirar su dinero en absoluto, o sólo podrá hacerlo si paga altos cargos.

- **Un estafador se hace pasar por una celebridad que puede multiplicar las criptomonedas que usted le envíe.** Pero no hay ninguna persona famosa que se esté comunicando con usted a través de los medios sociales. Es un estafador. Y si hace clic en un enlace inesperado que le envíen o si le envía criptomonedas al código QR de una supuesta celebridad, ese dinero va a parar directamente al bolsillo de un estafador y desaparece.

- **Un "enamorado" virtual quiere que usted le envíe dinero o criptomonedas para ayudarlo a invertir.** Eso es una estafa. Tan pronto como alguien que conozca en un sitio o aplicación de citas le pida dinero, o le ofrezca consejos de inversión, sepa que

es un estafador. Los consejos y el ofrecimiento de ayudarlo a invertir en criptomonedas no son otra cosa que estafas. Si le envía una criptomoneda, o cualquier otra forma de dinero, desaparecerá, y habitualmente no lo recuperará.

- **Los estafadores le garantizan que ganará dinero o le prometen que obtendrá altos rendimientos garantizados.** Nadie puede darle esas garantías. Y mucho menos en un breve período de tiempo. Y en lo que se refiere a inversiones en criptomonedas, no existe nada que sea de "bajo riesgo". Así que, si una compañía o persona le promete que obtendrá ganancias, es una estafa. Incluso si cuentan con el endoso de personas famosas o el testimonio de inversores felices. Eso es algo que se puede falsear fácilmente.
- **Los estafadores prometen dinero gratis**. Prometerán dinero en efectivo o criptomonedas gratis, pero las promesas de dinero gratis son siempre falsas.

- **Los estafadores hacen grandes declaraciones sin detalles o explicaciones.** Cualquiera sea la inversión, averigüe cómo funciona y pregunte a dónde irá su dinero. Los gerentes o asesores de inversiones honestos estarán dispuestos a compartir esa información y la respaldarán con detalles.

Imitadores de negocios, agencias del gobierno y oferentes de empleo

En una estafa perpetrada por personas que se hacen pasar por representantes de negocios, agencias del gobierno u oferentes de empleo, el estafador finge ser alguien en quien usted confía para convencerlo de que le envíe dinero mediante la compra y el envío de criptomonedas.

Los estafadores se hacen pasar por compañías reconocidas. Esto se presenta en oleadas, dependiendo del momento, y los estafadores podrían decir que trabajan para Amazon, Microsoft, FedEx, su banco o demás. Este tipo de estafador le enviará un mensaje de texto, un email o se comunicará por teléfono o a través de mensajes en los medios sociales, o tal vez coloque una alerta pop-up en su computadora. Podrían decirle que se produjo un

fraude en su cuenta, o que su dinero está en riesgo, y que, para resolver el problema, usted tiene que comprar criptomonedas y enviárselas. Pero eso es una estafa. Si hace clic en el enlace de un mensaje, responde la llamada o llama al número que aparece en la ventana pop-up, se comunicará con un estafador. (COMERCIO C. F., 2022)

6.0. Fraudes financieros con criptomonedas

Esquemas Ponzi o piramidales

Prometen **ganancias fijas o muy altas en poco tiempo** si inviertes en cierta criptomoneda o plataforma.

Te pagan los primeros "beneficios" con el dinero de nuevos usuarios.

Cuando no entran más personas, desaparecen con el dinero.

Falsos asesores financieros o traders

Se hacen pasar por expertos en criptomonedas, te contactan por redes o WhatsApp.

Te invitan a invertir en plataformas falsas o controladas por ellos.

Después de invertir, **no puedes retirar tu dinero** o te cobran "comisiones" para liberar fondos.

Plataformas de inversión falsas

Sitios web que imitan exchanges legítimos (como Binance, Coinbase) pero son falsos.

Te piden que deposites fondos o criptomonedas, y luego **desaparecen o bloquean tu acceso**.

A veces muestran gráficos, balances o ganancias falsos para parecer reales.

Apps fraudulentas

Aplicaciones móviles que parecen legítimas y están incluso en tiendas oficiales (Play Store, App Store).

Una vez que depositas fondos, **no permiten retirar** o desaparecen con tus activos.

Rug pull (tirón de alfombra)

Se lanza una nueva criptomoneda o token con gran publicidad.

Suben su precio artificialmente con promesas de utilidad futura.

Los creadores venden sus monedas de golpe y **hunden el precio a cero**, dejando a los inversores sin valor.

Phishing y robo de claves

Sitios web falsos o mensajes que te piden ingresar tu "frase semilla" o claves privadas.

Nunca debes compartir tus claves privadas: quien las tiene, tiene tus criptos.

Estafas románticas cripto

Te enamoran por redes sociales o apps de citas.

Luego te introducen al "mundo cripto" y te convencen de invertir con ellos.

Usan plataformas controladas o te convencen de hacer transferencias directas.

Falsos sorteos o giveaways

Prometen duplicar criptomonedas: *"Envíame 0.1 BTC y te devuelvo 0.2 BTC"*

Se hacen pasar por Elon Musk, influencers o cuentas famosas.

Se difunden por YouTube, Twitter/X, Instagram y Telegram.

6.1 Estafas electrónicas mediante cursos o certificados de estudio online

Las **estafas con cursos y certificados en línea** han crecido notablemente desde la pandemia de COVID-19, cuando millones de personas recurrieron a la educación digital. Estafadores y plataformas fraudulentas aprovecharon esta tendencia para **ofrecer cursos falsos, certificados sin validez o promesas educativas engañosas**.

Según el sitio web "Infobae", en la web existen Universidades Ficticias que ofrecen certificados de estudio, el sitio resume la forma de operar de dichas universidades en referencia a un informe realizado por la UNESCO, denominado: " *"Escuelas corruptas, universidades corruptas. ¿Qué se puede hacer?"*, la *Unesco* ya alertaba acerca de este lunar en el sistema educativo mundial. El informe aseguraba que la cantidad de universidades ficticias publicadas en internet se habían cuadruplicado y llegaban a un total de 800."

Los autores del informe, Jacques Hallak y Muriel Poisson, reconocieron que la irrupción de internet promovió el "contrabando" de diplomas, títulos y credenciales falsas, y

definieron el fraude académico como "la utilización de una institución pública para el enriquecimiento privado en el campo académico, especialmente en el ámbito de la investigación y la emisión de títulos de educación superior" (INFOBAE, s.f.)

6.2 Estafas con cursos y certificados en línea

Certificados sin validez oficial

Te ofrecen un curso “avalado” o “certificado” por universidades o instituciones reconocidas, pero es falso.

El certificado no tiene ningún valor legal ni académico.

Ejemplo: Un curso que dice estar “avalado por Harvard” pero no tiene relación con la universidad.

Cursos de pago que nunca se entregan

Sitios o redes sociales ofrecen cursos “premium” con temarios atractivos.

Pagas con tarjeta o transferencia y **no recibes acceso al curso ni respuestas**.

Suplantación de plataformas reales

Clonan sitios conocidos (como Coursera, Udemy, EdX) para robar tus datos o cobrar por cursos inexistentes.

A menudo usan dominios parecidos (como coursera-certificado.com).

Cursos con promesas exageradas o falsas

Prometen: “gana $5000 al mes con este curso”, “trabaja en Google tras finalizar”, o “certificado garantizado sin examen”.

Se enfocan más en **vender el curso** que en enseñar algo real.

Phishing educativo

Correos o anuncios falsos que dicen: *“Has sido seleccionado para una beca o curso gratuito”*.

Te piden completar formularios con **datos personales o bancarios**.

Venta de certificados sin cursar

Sitios que te ofrecen directamente certificados a cambio de dinero sin necesidad de hacer el curso.

Esto puede ser **ilegal** si se usa para engañar a empleadores o instituciones.

Cursos técnicos falsos

Cursos de programación, ciberseguridad, trading, etc., con contenido pobre o robado de internet.

Te prometen habilidades laborales reales, pero no hay estructura ni soporte.

6.3 Estafas de soporte técnico

Las **estafas de soporte técnico** son un tipo de fraude digital en el que los delincuentes se hacen pasar por personal de soporte de empresas tecnológicas (como Microsoft, Google, Apple o proveedores de antivirus) para **asustar a la víctima y obtener acceso remoto a su dispositivo o robar dinero e información personal**.

Estas estafas han aumentado especialmente **post-COVID-19**, aprovechando que más personas trabajan y estudian desde casa, a menudo sin conocimientos técnicos avanzados.

¿Cómo funcionan?

Los estafadores pueden hacerse pasar por técnicos de una compañía tecnológica reconocida, por ejemplo, Microsoft. Usan muchos términos técnicos para convencerlo de que los problemas de su computadora son reales. Le pueden pedir que abra algunos archivos o que escanee su computadora — y luego le dicen que esos archivos o los resultados del escaneo indican un problema (que en realidad no existe**).** (COMERCIO C. F., 2022)

El estafador:

1. Se comunica contigo por **teléfono, mensaje, correo electrónico o página emergente (pop-up)**.
2. Asegura que tu dispositivo está infectado o comprometido.
3. Te pide instalar un programa para "ayudarte" (como AnyDesk, TeamViewer o similares).
4. Una vez que tiene acceso remoto:
    - Roba archivos o contraseñas.
    - Instala malware o ransomware.

- Solicita pagos por servicios inexistentes.

6.4. Formas comunes de estafa

Llamadas falsas

- Te llaman diciendo: *"Somos de Microsoft, detectamos un virus en tu PC"*, o *"su licencia está vencida"*.
- Te piden que sigas instrucciones, accedas a una web o instales software.

Pop-ups o ventanas emergentes

- Navegando en internet aparece un mensaje tipo: *"¡Alerta! Tu computadora ha sido infectada. Llama a este número: 800-XXX-XXXX"*
- La ventana **simula ser de Microsoft o de tu antivirus**, y bloquea tu pantalla.

Correos o mensajes falsos

- Correos diciendo que tu cuenta está en riesgo o que deben verificar actividad sospechosa.
- Contienen enlaces que instalan software malicioso o redirigen a páginas falsas de soporte.

Aplicaciones móviles de "soporte"

- Aplicaciones falsas en Google Play o links externos que se hacen pasar por herramientas oficiales.
- Una vez instaladas, permiten controlar tu teléfono de forma remota.

¿A quién apuntan?

- Personas mayores o con poca experiencia digital.
- Empleados en teletrabajo.
- Usuarios preocupados por la seguridad de sus dispositivos.

Señales de alerta

- Te contactan **sin que tú lo hayas solicitado**.
- Usan **lenguaje urgente o amenazante** (“si no actuamos ahora, perderás todo”).
- Te piden instalar software remoto o compartir tu pantalla.
- Te exigen pagos inmediatos por “soluciones técnicas”.

6.4. Estafas de alquiler o venta de inmuebles

Las **estafas de alquiler o venta de inmuebles** han aumentado considerablemente con la digitalización de procesos inmobiliarios tras la pandemia del COVID-19. Los estafadores aprovechan portales web, redes sociales y aplicaciones de mensajería para **engañar a personas que buscan alquilar o comprar una vivienda**, especialmente cuando hay urgencia o necesidad de mudanza.

En primer lugar, **una estafa común que suele producirse en el proceso de compra o alquiler de una propiedad es el caso de los anuncios fraudulentos.**

Estos anuncios engañosos pueden presentar propiedades inexistentes, en condiciones de alquiler engañosas o ventas ficticias, con el fin de sacar dinero o información personal a personas que no lo sospechan.

Otro esquema prevalente es la aparición de agencias inmobiliarias fantasma, que operan con el único propósito de engañar a los clientes, **utilizando información falsa de la agencia y promesas falsas para atraer a sus víctimas**.

Por último, el alquiler o venta no autorizados de una propiedad por un estafador que se hace pasar por el propietario legítimo, a pesar de no tener derecho legal a la propiedad, también es una situación lamentablemente frecuente. (FLORES, 2024)

6.4.1. Modalidades más comunes

Propiedad inexistente o suplantada

- El estafador publica un anuncio con fotos reales (robadas de otras páginas).
- Dice ser el propietario o agente, pero **la propiedad no está en renta o no existe**.
- Pide una **seña, adelanto o reserva por transferencia bancaria**, y luego desaparece.

Frases típicas:
"Estoy en el extranjero, pero puedo enviarte las llaves por paquetería"
"Necesito asegurar que eres un inquilino serio, deposita primero"

Fotografías falsas o manipuladas

Publican imágenes muy atractivas a un precio sospechosamente bajo.

- Cuando vas al lugar (si existe), la propiedad **no se parece** o está ocupada.

Suplantación de agentes inmobiliarios

- Usan identidades, logotipos o credenciales falsos de inmobiliarias reales.
- Te contactan por WhatsApp, Facebook o correos.
- Ofrecen condiciones demasiado favorables y presionan para pagos rápidos.

Venta fraudulenta de propiedades ajenas

- Se falsifican documentos de propiedad, escrituras o identificaciones.
- La víctima paga un anticipo, firma documentos, y **descubre que el "vendedor" no era el dueño real**.

Falso dueño en el extranjero

- Alegan estar fuera del país por trabajo o misión diplomática.
- Ofrecen enviar contrato y llaves por servicios como Airbnb, DHL o FedEx *previo depósito*.
- La transacción es simulada y **la propiedad nunca se entrega**.

Alquiler temporal fantasma (Airbnb, Booking, etc.)

- Usan plataformas de reservas para crear anuncios falsos o cancelan justo después del pago.

- En algunos casos, **copian perfiles legítimos** y modifican enlaces o datos bancarios.

Señales de alerta

- Precio muy bajo para la zona o condiciones del inmueble.
- El supuesto dueño o agente **evita mostrar la propiedad físicamente**.
- Solo se comunican por WhatsApp o email, y **evitan llamadas o videollamadas**.
- Exigen dinero anticipado antes de firmar un contrato o visitar el lugar.
- Te piden usar métodos de pago poco rastreables (transferencias internacionales, criptomonedas, servicios de envío de dinero).

CONCLUSIONES

- **LA PANDEMIA DEL COVID-19, GENERÓ UN IMPACTO ECONÓMICO A NIVEL MUNDIAL:**

La paralización casi total de la economía mundial, dio paso a una crisis global y un desabastecimiento a nivel nacional e internacional de productos y servicios para uso y consumo humano.

- **MUTACIÓN DEL COMERCIO DEBIDO AL AISLAMIENTO Y DISTANCIAMIENTO SOCIAL**

El ser humano por naturaleza es ingenioso y a pesar de las dificultades, siempre busca alternativas, lo que generó que a pesar del distanciamiento social y el aislamiento se encontraran nuevos métodos de comunicación y de abastecimiento de bienes y servicios esenciales y no esenciales para la subsistencia humana.

- **CRECIMIENTO DEL COMERCIO ELECTRÓNICO:**

El comercio electrónico ya existía antes de la pandemia del covid-19 y era una forma mercantil en ascenso que tuvo un aumento considerable debido a la pandemia del covid-19 y gracias a las redes sociales y plataformas electrónicas.

- **NEGOCIO Y DELITOS**

El incremento del comercio electrónico, también conlleva el aumento en el flujo de dinero en dicha actividad y hay que tener en cuenta que "toda actividad lucrativa es atractiva a la delincuencia", que se las ingenia para incursionar en aquellas áreas en donde se mueve dinero o bienes de valor económico. Es dable inferir que: ***"El aumento del comercio electrónico, genera un aumento del flujo de dinero y bienes por internet y consecuentemente aumenta la criminalidad informática."***

- **MUTACIÓN DE LAS ESTAFAS ELECTRÓNICAS POST COVID-19**

Las estafas informáticas han tenido una notable mutación posterior a la pandemia del Covid-19, el realce de las redes sociales y el expansionismo de la inteligencia artificial han permitido que la criminalidad cibernética pueda generar diferentes modos de engañar a sus víctimas y obtener provecho económico.

REFERENCIAS

360, N. D. (O1 de DICIEMBRE de 2023). *DELITOS INFORMÁTICOS EN MEXICO. CONOZCA LAS LEYES Y LAS MULTAS.* Obtenido de ITMASTERSMAG.COM: https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

Argentina, G. d. (2 de mayo de 2024). *Argentina.gob.ar.* Obtenido de Argentina.gob.ar: https://www.argentina.gob.ar/justicia/derechofacil/leysimple/delitos-informaticos#titulo-4

ARGENTINA, G. D. (DICIEMBRE de 2024). *ARGENTINA.GOB.AR*. Obtenido de ARGENTINA.GOB.AR: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing#:~:text=La%20palabra%20phishing%20quiere%20decir,la%20identidad%20de%20esas%20personas

ARMERO, R. (13 de julio de 2024). *www.businessinsider*. Obtenido de www.businessinsider: https://www.businessinsider.es/tecnologia/estas-son-estafas-inteligencia-artificial-utilizadas-como-puedes-enfrentarte-ellas-1394135

CARRERA, D. P. (2004). DERECHO PENAL DE LOS NEGOCIOS. En D. P. OTRO, *DERECHO PENAL DE LOS NEGOCIOS* (pág. 1). BUENOS AIRES: ASTREA.

CENIT, P. D. (6 de ENERO de 2025). *ELCENIT.COM.SV*. Obtenido de ELCENIT.COM.SV: https://elcenit.com.sv/2025/01/06/este-9-de-enero-entran-en-vigor-las-fotomultas-en-el-salvador/

CENTRAL, C. R. (27 de julio de 2023). *blog.rural central.es*. Obtenido de blog.rural central.es: https://blog.ruralcentral.es/la-estafa-digital-mas-frecuente-en-espana-el-robo-de-identidad/

CHILE, B. D. (s.f.). *www.bcn.cl.* Obtenido de www.bcn.cl: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf

COLOMBIA, C. D. (2 de MAYO de 2024). *GOV.CO.* Obtenido de GOV.CO: https://www.senado.gov.co/index.php/el-senado/noticias/4660-senado-solidario-con-victimas-de-fraude-digital#:~:text=Entre%20las%20leyes%20que%20aprob%C3%B3,de%202023%20(Prensa%20Senado).

COMERCIO, C. F. (mayo de 2022). *www.consumidor.ftc.gov*. Obtenido de www.consumidor.ftc.gov: https://consumidor.ftc.gov/articulos/lo-que-hay-que-saber-sobre-las-criptomonedas-y-las-estafas

COMERCIO, S. D. (2 de mayo de 2024). *www.sic.gov.co.* Obtenido de www.sic.gov.co: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

COMPETENCIA, S. D. (30 de enero de 2019). *www.sc.gob.sv*. Obtenido de www.sc.gob.sv: https://www.sc.gob.sv/index.php/sala_multimedia/opinionnormativa-sc-003-s-on-r-2019/

CREUS, C. (1998). *DERECHO PENAL PARTE ESPECIAL, TOMO I.* BUENOS AIRES, ARGENTINA: EDITORIAL ASTREA.

CURIOSAWEB. (s.f.). *www.curiosaweb.com*. Obtenido de www.curiosaweb.com: https://curiosaweb.com/la-historia-del-correo-electronico-una-revolucion-en-la-comunicacion/?damemas_lectura=1

diputados.gob.mx. (16 de abril de 2024). *diputados.gob.mx.* Obtenido de diputados.gob.mx: https://www.diputados.gob.mx/LeyesBiblio/pdf/LIC.pdf

DROIDERS. (s.f.). *www.droiders.com*. Obtenido de www.droiders.com: https://www.droiders.com/aplicaciones-de-mensajeria/#:~:text=Las%20aplicaciones%20de%20mensajer%C3%ADa%20son%20programas%20inform%C3%A1ticos%20que,voz%2C%20im%C3%A1genes%2C%20v%C3%ADdeos%20y%20otros%20tipos%20de%20archivos.

E&N, R. (2025). *revistaeyn.com*. Obtenido de revistaeyn.com: https://www.revistaeyn.com/tecnologia-cultura-digital/las-estafas-mas-comunes-en-las-compras-online-y-como-protegerse-FB25712777

ECONOMIPEDIA.COM. (s.f.). *www.economipedia.com*. Obtenido de https://economipedia.com/definiciones/estafa-piramidal.html

ESPAÑOLA, R. A. (s.f.). *www.dle.rae.es*. Obtenido de www.dle.rae.es: https://dle.rae.es/comercio

EUROPA, C. D. (23 de noviembre de 2001). *rm.coe.int*. Obtenido de rm.coe.int: https://rm.coe.int/16802fa403

FACCHIN, J. (s.f.). *el blog de Jose Facchin*. Obtenido de el blog de Jose Facchin: https://josefacchin.com/facebook-que-es-como-funciona/

FINANZAS, M. Y. (18 de MARZO de 2021). *MERCADOS Y FINANZAS.COM*. Obtenido de MERCADOS Y FINANZAS.COM: HTTPS://MERCADOSYFINANZAS.COM

FLORES, J. G. (09 de septiembre de 2024). *www.confilegal.com*. Obtenido de www.confilegal.com: https://confilegal.com/20240910-opinion-cuidado-las-estafas-inmobiliarias-acechan-como-protegerte-de-fraudes-al-comprar-o-alquilar/

FRANCISCO MUÑOZ CONDE, Y. O. (2004). *DERECHO PENAL PARTE GENERAL* . VALENCIA: TIRANT LO BLANCH.

GEEKNETIK. (s.f.). *www.geeknetik.es*. Obtenido de www.geeknetik.es: https://www.geeknetic.es/Instagram/que-es-y-para-que-sirve

González, J. A. (junio de 2013). *eprints.uanl.mx.* Obtenido de eprints.uanl.mx: http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

GUADALAJARA, U. D. (s.f.). *biblioteca.udgvirtual.udg.mx.* Obtenido de biblioteca.udgvirtual.udg.mx: http://biblioteca.virtual.udg.mx/jspui/bitstream/123456789/3088/1/resumen%20

Hutt Herrera, H. (2012). LAS REDES SOCIALES: UNA NUEVA HERRAMIENTA DE DIFUSION . *REVISTAS.UCR*, 4.

Infobae. (2 de mayo de 2024). *infobae.com.* Obtenido de infobae.com: https://www.infobae.com/colombia/2024/04/23/internet-y-el-aumento-de-fraudes-digitales-en-colombia-conozca-que-clase-de-sitios-web-usan-los-delincuentes/

INFOBAE. (s.f.). *www.infobae.com*. Obtenido de www.infobae.com: https://www.infobae.com/tendencias/2016/10/05/fraude-educativo-las-universidades-ficticias-que-operan-en-internet/

issu. (s.f.). Obtenido de iss.

ISSUU. (31 de JULIO de 2021). *ISSUU*. Obtenido de ISSUU: https://issuu.com/derechoynegocios/docs/edici_n_112_dyn_web/22?fbclid=IwY2xjawIKFOhleHRuA2FlbQIxMQABHRZwLVzt3B_IZhWZQCC0Iz4NJn1XWP1JOrvtBCe9NGdjSYygOBYdgMuDLA_aem_lDZr1EiIBHwtI-co5Pebnw&sfnsn=wa

JURIDICO, D. P. (2023). *DPEJ PANHISPANICO*. Obtenido de DPEJ PANHISPANICO: https://dpej.rae.es/lema/%C3%A1nimo-de-lucro

LAW&TRENDS. (s.f.). *law&trends.com*. Obtenido de law&trends.com: https://www.lawandtrends.com/noticias/penal/el-romance-scam-o-estafa-amorosa-1.html#gsc.tab=0

LEGAL, T. I. (s.f.). *TODO INFO LEGAL*. Obtenido de TODO INFO LEGAL: https://todoinfolegal.com/diferencia-entre-responsabilidad-limitada-e-ilimitada/#:~:text=La%20responsabilidad%20limitada%20e%20ilimitada%20son%20dos%20conceptos,por%20las%20deudas%20y%20obligaciones%20de%20la%20empresa.

MENJIVAR, M. A. (2022). LA EXTINCION DE DOMINIO EN EL SALVADOR. En M. A. MENJIVAR, *LA EXTINCION DE DOMINIO EN EL SALVADOR* (pág. 33). SAN SALVADOR: CUSCATLECA.

MUNDO, D. E. (LUNES de DICIEMBRE de 2021). *DIARIO. EL MUNDO.SV*. Obtenido de DIARIO. EL MUNDO.SV: HTTPS://DIARIO EL MUNDO.SV

MUÑOZ CONDE, F. (2004). *DERECHO PENAL PARTE ESPECIAL* . VALENCIA, ESPAÑA: TIRANT LO BLANCH.

SAIN, G. (s.f.). EVOLUCION HOSTORICA DE LOS DELITOS INFORMATICOS . *REVISTA PENSAMIENTO PENAL*, 1.

Salud, O. R. (11 de marzo de 2020). *paho.org*. Obtenido de paho.org: https_//www.paho.org/es/noticias

SALVADOR, A. L. (01 de DICIEMBRE de 2022). *ASAMBLEA.GOB.SV*. Obtenido de ASAMBLEA. GOB.SV: HTTPS//ASAMBLEA.GOB.SV

SALVADOR, A. L. (s.f.). *portaldetransparecia.fgr.gob.sv*. Obtenido de portaldetransparecia.fgr.gob.sv: https://portaldetransparencia.fgr.gob.sv/documentos/Ley%20Especial%20contra%20Delitos%20Inform%C3%A1ticos%20y%20Conexos.pdf

SANTANDER, B. (s.f.). *www.bancosantander.es*. Obtenido de www.bancosantander.es: https://www.bancosantander.es/glosario/ransomware#:~:text=El%20ransomware%2C%20en%20inform%C3%A1tica%2C%20es,%2C%20bloqueando%20la%20pantalla%2C%20etc.

SCAMADVISER. (17 de NOVIEMBRE de 2020). *SCAMADVISER.COM*. Obtenido de SCAMADVISER.COM: https://www.scamadviser.com/es/articles/las-10-principales-estafas-en-linea-de-2020

Sean Lyngaas, H. R. (14 de MARZO de 2023). El FBI dice que se perdieron US$ 10.000 millones por fraude en línea en 2022 a medida que aumentaron las estafas de criptoinversión. *CNN*, págs. https://cnnespanol.cnn.com/2023/03/14/fbi-perdieron-10000-millones-dolares-fraude-linea-2022-estafas-criptoinversion-trax/.

SIGNIFICADOS, E. (s.f.). *SIGNIFICADOS.COM*. Obtenido de SIGNIFICADOS.COM: https://www.significados.com/algoritmo/

SV, Q. P. (15 de ENERO de 2025). *QUEPASASV*. Obtenido de QUEPASASV: https://quepasasv.com/vmt-alerta-sobre-estafa-con-falsas-fotomultas-en-el-salvador/#:~:text=El%20Viceministerio%20de%20Transporte%20%28VMT%29%20ha%20emitido%20una,usuarios%20con%20el%20fin%20de%20obtener%20pagos%20fraudulentos.

swissinfo.ch. (24 de mayo de 2023). *swissinfo.ch*. Obtenido de swissinfo.ch: https://www.swissinfo.ch/spa/la-sociedad-de-internet-de-china-alerta-sobre-el-aumento-del-fraude-impulsado-por-ia/48536738

TELLEZ, A. G. (s.f.). *MANUAL DE DERECHO DE LAS OBLIGACIONES CIVILES.* UNIVERSIDAD IBEROAMERICANA DE PUEBLA.

transparencia.gob.sv. (11 de marzo de 2020). *transparencia.gob.sv*. Obtenido de transparencia.gob.sv: https://transparencia.gob.sv

VASQUEZ, D. P. (2004). *DERECHO PENAL DE LOS NEGOCIOS.* BUENOS AIRES, ARGENTINA: ASTREA.

VELADO, R. L. (s.f.). *INTRODUCCION AL ESTUDIO DEL DERECHO MERCANTIL* .

VLEX. (s.f.). *vlex.com*. Obtenido de vlex.com: https://sv.vlex.com/vid/698077109

WIKIHOW. (s.f.). *www.wikihow.com*. Obtenido de www.wikihow.com: https://es.wikihow.com/detectar-las-estafas-por-WhatsApp

ANEXOS

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

Objetivo General: Identificar las nuevas modalidades de Estafas por medios electrónicos o redes sociales como consecuencia del aumento del comercio electrónico desde la pandemia de COVID-19.

Objetivo Específico 1	**Variable**	**Definición conceptual u operativa de cada variable**	**Indicadores**	**Cómo se recogerán los datos (Técnicas)**	**Que preguntas si es encuesta o entrevista o que acciones se harán si es otra forma de recolección de datos**	**Fuente de donde se recolectará la información**
Clasificar las modalidades de oferta, demanda, negocia	Variable 1 Objetivo 1 Modalidades de Oferta(medios	Oferta: Conjunto de bienes o mercancias que se presentan a traves de publicidad en redes sociales y	-Bienes y Mercancías. -Publicidad en redes sociales	- Gestion institucional de informacion	- ¿Cuales son los bienes y mercancias por los que se han	Defensoria del Consumidor (portal de trasparenc

ción y adquisición de bienes y servicios a través de medios informáticos en El Salvador.	informaticos) Modalidades de Demanda(medios informaticos) Adquisicion de bienes y servicios (medios informaticos) .	otras plataformas electronicas, en el mercado virtual, con un precio concreto,u otros insentivos para persuadir al consumidor. (Elaboración Propia) Demanda: Cuantia global de las compares de bienes y servicios realizados o previstos en una colectividad.	-Publicidad en redes electrónicas -Mercado Virtual -Incentivos para persuadir - Consumidor. -Bienes materiales(objetos) -Bienes inmateriales (Derechos u obligaciones susceptibles	-Gestion institucional de informacion	iniciado procesos en esta unidad? (comercio electronico) -¿Como saben las redes sociales lo que quiero comprar? (dentro del marco de las teorias) -¿Cuales son las platafor mas o redes sociales mas utilizadas, para adquirir	ia, solicitud)

		(f.Econ. del.rae.es) Bienes: Todo aquello de carácter material o inmaterial suceptible de tener un valor (Diccionario Juridico, Mabel Goldstein, 2008) Servicios:Organización y	de un valor pecuniario) - Organización (persona jurídica) -Personal (persona natural) -Cuidar y satisfacer necesidades		bienes o mercancias? -¿Como recibio la oferta del producto o mercancia? -¿Que tipo de rubro prefiere pedir o comercializar en linea, los bienes o los servicios? -Sobre que objeto recaen mas las	Centro de Documentación Judicial Portal de trasparaencia de la FGR.

		personal destinados a cuidar intereses o satisfacer necesidades del publico o de alguna entidad (Diccionario Juridico, Mabel Goldstein, 2008)			estafas electronicas, en los bienes o en los servicios ? -¿Cual es el perfil de los clientes victimas que son objeto de engaño que denuncian legalmente?	
	Variable 2 Objetivo 1					

Cronograma de actividades.

En un diagrama de Gantt, se colocarán las diversas actividades correspondientes al desarrollo de la investigación, esto a fin de mostrar los tiempos determinados para el desarrollo del estudio.

Nº	ACTIVIDADES	Marzo		Abril				Mayo				Junio				Julio			
		3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Recopilación, clasificación y sistematización de la información sobre el problema	x	x	x	x														
2	Elaboración del Proyecto de trabajo				x	x													
3	Entrega de proyecto de investigación						x												
4	Proceso de elaboración del						x	x	x	x	x	x							

	Protocolo de investigación																	
5	Avance del Protocolo											x	x					
6	Elaboración y entrega de informe final del Protocolo													x	X	x	x	x	
7	Desarrollo del proceso de investigación																	x	x

PRESUPUESTO

Se mencionarán los costos de la investigación generando una estimación de la información según los rubros de gastos que se tendrán.

RECURSOS

- Humanos: Dos estudiantes que forman el grupo investigador.

- Materiales:

  Dos computadoras portátiles.

  Dos computadoras con acceso libre a Internet.

  Dos memorias USB de 16 Gigabytes cada una.

  Dos Celulares.
- Económicos
- Humanos

Cantidad	*Nombre*	**Costo unitario**	**Costo total por 4 meses**
1	Asesor particular	$300.00 mensuales	$ 1,200.00
1	Lorena Novoa mensualidad	$100.00 mensuales	$ 400.00
1	Miguel Cárcamo mensualidad	$100.00 mensuales	$ 400.00
		Subtotal 1	**$ 2,000.00**

- Materiales

Cantidad	Rubro	Costo Unitario	Costo Total
3	Resmas de papel bond	$ 4.50	$ 13.50
1	Cartucho de tinta negra para impresor	$ 25.00	$ 25.00
1	Cartucho de tinta color para impresor	$ 30.00	$ 30.00
1	Saldo para el celular	$ 15.00	$ 15.00
2	Cuaderno de apuntes	$ 1.75	$ 5.25
3	Folders y Fastener	$ 0.25	$ 0.75
2	Memoria USB 16GB	$ 6.50	$ 13.00
		Subtotal 2	**$102.50**

- Imprevistos y varios

Varios	**Cantidad por día**	**Costo total por 4 meses**
Transporte/gas	$ 20.00	$ 690.00
Alimentación	$ 10.00	$ 390.00
Imprevistos	$ 150.00	$ 150.00
	Subtotal 3	**$1,230.00**

- Financieros

Subtotal 1	$**2,000.00**
Subtotal 2	$**102.50**
Subtotal 3	$**1,230.00**
TOTAL	**$ 3,332.50**

FORMATO DE SOLICITUD

FISCALÍA GENERAL DE LA REPÚBLICA DE EL SALVADOR

PRESENTE.-

MIGUEL ANGEL CARCAMO IRAHETA, mayor de edad, Abogado y Notario, del Domicilio de Zacatecoluca, Departamento de La Paz; con Documento Único de Identidad numero 03976476-2; a ustedes con el debido respeto: **MANIFIESTO:**

Que actualmente soy egresado de la maestría en Derecho Penal Económico de la Universidad de El Salvador y me encuentro elaborando mi tesis con el tema denominado " LAS MODALIDADES DEL DELITO DE ESTAFA POR MEDIOS INFORMÁTICOS COMO CONSECUENCIA DE LA EVOLUCIÓN DEL COMERCIO ELECTRÓNICO DESDE LA PANDEMIA DE COVID 19".

Que para sustentar mi investigación es necesario obtener datos oficiales de vuestra institución con la siguiente información: a) el número de Denuncias por Delito de Estafa por medios informáticos recibidas en vuestra institución del año 2020 al 2023; b) el numero de Estafas en modalidad electrónicas que han sido judicializadas desde el año 2020 a 2023; c) el numero de condenas por Estafas Electrónicas obtenidas por vuestra institución desde el año 2020 a 2023.

Por todo lo antes expuesto, de conformidad con los artículos 3, 61 y 66 de la Ley de Acceso a la Información Publica os **PIDO**:

1. ADMITIRME EL PRESENTE ESCRITO
2. SE ME EXTIENDA INFORME POR MEDIO DE CORREO ELECTRÓNICO EN EL QUE CONSTE LA SIGUIENTE INFORMACIÓN: A) EL NÚMERO DE DENUNCIAS POR DELITO DE ESTAFA POR MEDIOS INFORMÁTICOS RECIBIDAS EN VUESTRA INSTITUCIÓN DEL AÑO 2020 AL 2023; B) EL

NÚMERO DE ESTAFAS EN MODALIDAD ELECTRÓNICAS QUE HAN SIDO JUDICIALIZADAS DESDE EL AÑO 2020 A 2023; C) EL NUMERO DE CONDENAS OBTENIDAS POR ESTAFAS ELECTRÓNICAS OBTENIDAS POR VUESTRA INSTITUCIÓN DESDE EL AÑO 2020 A 2023.

Señalo para recibir notificaciones mi Oficina Jurídica en Avenida Narciso Monterrey, número 23, Barrio el Centro, Zacatecoluca, Departamento de La Paz, con telefax 2334-1574, WhatsApp 76822579 y al correo electrónico **mikel9930@hotmail.com** y; por lo antes expuesto

San Salvador_____de _____2024.

DEFENSORÍA DEL CONSUMIDOR DE EL SALVADOR

PRESENTE.-

LORENA ELIZABETH NOVOA POLANCO, de treinta y siete años de edad, Abogada, del Domicilio de Santa Ana, Departamento de Santa Ana; con Documento Único de Identidad numero 03533807-2; a ustedes con el debido respeto: **MANIFIESTO:**

Que actualmente soy egresada de la maestría en Derecho Penal Económico de la Universidad de El Salvador y me encuentro elaborando mi tesis con el tema denominado " LAS MODALIDADES DEL DELITO DE ESTAFA POR MEDIOS INFORMÁTICOS COMO CONSECUENCIA DE LA EVOLUCIÓN DEL COMERCIO ELECTRÓNICO DESDE LA PANDEMIA DE COVID 19".

Que para sustentar mi investigación es necesario obtener datos oficiales de vuestra institución con la siguiente información: **EL NÚMERO DE DENUNCIAS RECIBIDAS DE LOS AÑOS 2020 A 2023, POR VIOLACIÓN A LA LEY DE PROTECCIÓN AL CONSUMIDOR MEDIANTE LA REALIZACIÓN DE ACTIVIDADES DE COMERCIO ELECTRÓNICO.**

Por todo lo antes expuesto, de conformidad con los artículos 3, 61 y 66 de la Ley de Acceso a la Información Pública os PIDO:

1. ADMITIRME EL PRESENTE ESCRITO

SE ME EXTIENDA INFORME POR MEDIO DE CORREO ELECTRÓNICO EN EL QUE CONSTE LA SIGUIENTE INFORMACION: EL NÚMERO DE DENUNCIAS RECIBIDAS DE LOS AÑOS 2020 A 2023, POR VIOLACIÓN A LA LEY DE PROTECCIÓN AL CONSUMIDOR MEDIANTE LA REALIZACIÓN DE ACTIVIDADES DE COMERCIO ELECTRÓNICO.

Señalo para recibir notificaciones mi, WhatsApp 7514-6556 y al correo electrónico **lorena_0422@hotmail.com**

San Salvador_____de _____2024.