UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

(P E T A E N G)

TRABAJO DIRIGIDO

(Para optar el Titulo Académico de Licenciatura en Derecho)

"ANÁLISIS DEL DELITO DE ESTAFA DIGITAL EN EL ESTADO PLURINACIONAL DE BOLIVIA"

POSTULANTE : PERCY ORSHAK VILLAZON SUSTACH

TUTOR : Dr. LUIS FERNANDO ZEGARRA CASTRO

La Paz - Bolivia

2021

Dedicatoria

Este trabajo dedico a mis Padres Franklin y Ana,

Quienes con su inmenso amor,

Siempre me enseñaron a aprender de los fracasos y disfrutar de los aciertos,

Andar por la vida por el camino de la bondad y la justicia,

A mi esposa Elvira quien me enseño a ser una mejor persona a su lado,

A mis hijos,

Jeshak Paolo, Percy Alejandro, y Matías Dylan, Por su inconmensurable cariño.

Agradecimiento

En primer lugar, quiero agradecer a Dios por permitirme culminar esta etapa de mi vida, a mi tutor Dr. Luis Zegarra Castro por su paciencia y sus buenos consejos, a las autoridades universitarias quienes nos allanan el camino que nos permitirá ingresar a la vida profesional y a todas las personas que directa o indirectamente me han colaborado para conseguir lo que me he propuesto.

Tabla de contenido

Resumen.-
Toda actividad humana de carácter económico financiero en la actualidad, está enmarcada en el conocimiento y manejo de tecnologías informáticas, las relaciones económicas sociales de nuestra época, influidas en gran parte por la pandemia Covid -19, han sido factor de un impulso de desarrollo de la tecnología informática a distancia, para poder acceder e interactuar entre las personas y las instituciones.

Estas circunstancias, también han sido causales del incremento de varios delitos informáticos, como es la Estafa Digital, motivo de esta investigación, en el que se explora todos los alcances y resultados de dicha actividad delictiva, que se ha expandido a nivel global sin restricción alguna, y que gracias a la tecnología informática muchos de los sujetos activos del delito informático , tuvieron un instrumento que ayuda su anonimato en la comisión de estos delitos , a la par la falta de normativa que tipifique una gran cantidad de variaciones de este tipo de delito de estafa digital, hallándose las personas afectadas, en un verdadero estado de indefensión y muy vulnerables ante la pérdida de su patrimonio.

Es de preocupación de esta investigación, establecer, recursos normativos, para futuras tipificaciones en el ámbito del derecho informático y el derecho penal ya que las tecnologías van cambiando a pasos agigantados para bien o para mal en el caso de los ciberdelincuentes que en su mayoría están adelantados a la jurisdicción estatal disfrutando de una total impunidad.

1. Introducción.-

Actualmente la población en su conjunto a nivel mundial, está superando a la peor pandemia Covid-19, en la historia de la humanidad, en el cual estamos obligados a interaccionar entre personas e instituciones de forma virtual o telemática, en los aspectos necesarios para el desarrollo social, como las transacciones financieras, pagos de deudas, pagos de servicios a entidades financieras y entidades públicas, transacciones entre particulares, movimientos de cuentas bancarias, envío de remesas del exterior y todo lo relacionado con el intercambio monetario, llegando a ser muy vulnerables las personas, con este tipo de delitos.

Cuando hablamos de ciberdelito se hace referencia a un tipo de delito, ya sea tradicional o propio de la sociedad de la información, generada por las tecnologías que ésta aporta, fundamentalmente en el internet.

El manejo informático en sí no es un delito, de aquel que utiliza un ordenador o una computadora, sino de aquel que emplea las redes informáticas u otros medios telemáticos para cometer delitos de estafa digital.

No obstante, el desarrollo de las nuevas tecnologías, además de fomentar las posibilidades al alcance del delincuente, también proporciona poderosas herramientas de investigación a los poderes públicos.

Pese a todas las oportunidades positivas que ofrece la red global, también ha creado oportunidades para estafadores llegando a ser uno de los más grandes problemas de la red.

Hace años, un ladrón atracaba un banco y robaba un millón de Dólares; ahora, un estafador especializado en manejo de la informática, sin necesidad de salir de su casa, puede estafar un dólar a un millón de personas.

Esta nueva realidad conlleva una problemática propia en la investigación de tales hechos como el análisis de estafa digital en el Estado Plurinacional de Bolivia.

Este tipo de conductas ilícitas que se planifican y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información, presentan a los efectos de su investigación y/o enjuiciamiento, singularidades y dificultades para su descubrimiento y persecución, así como para la identificación de las personas responsables de estos comportamientos ilícitos.

No se puede ignorar la vulnerabilidad de las personas por el riesgo de impunidad de muchas de estas conductas, precisamente por la escasa e imperceptible cuantía de desvió de dinero de alguno de estos fraudes que determina que las víctimas opten por no denunciar el delito, que ponderen el perjuicio económico sufrido con las molestias e inconvenientes que les puede suponer, interponer una denuncia e iniciar, así, un procedimiento penal.

Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo tipo y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros.

En definitiva, con la aparición del ciberdelito de estafa digital, el Derecho Penal se enfrenta a una criminalidad progresivamente más lesiva, que requiere a su vez los necesarios instrumentos procesales para hacerle frente y que esté a su vez no quede en la impunidad.

1.1. Diseño De La Investigación.-

La presente investigación aplica métodos y técnicas elegidos por el investigador para combinarlos lógicamente para que el problema de la investigación sea desarrollado de manera eficiente.

1.2. Enunciado Del Tema.-

Análisis del delito de estafa digital en el Estado plurinacional de Bolivia

1.3. Identificación Del Problema.-

La falta de normativa adecuada a este tipo de delito moderno, como es la Estafa Digital, hace que no sean imputables ante la ley por falta de elementos que conforman el delito con las diferentes figuras delictivas del código penal,

El Estado tutela todos los bienes jurídicos como la función pública, la salud la propiedad privada, el derecho internacional, la tranquilidad pública, el bienestar social, el matrimonio, la familia la seguridad interna y externa del Estado, el Estado civil , económico nacional y el turismo.

Hay figuras que hay que tipificarlas, y por esto el código penal va cambiando, se va adecuando al uso de las nuevas tecnologías de información y comunicación

Todas las acciones delictivas atentatorias, son susceptibles de un determinado proceso para una sanción.

1.4. Problematización.-

1.4.1. ¿Qué Sabemos Del Delito De Estafa Digital?

Un delito de estafa digital consiste en engañar a otro con ánimo de lucro, mediante el uso de instrumentos digitales, sistemas informáticos, induciendo a la víctima a realizar un acto de disposición patrimonial en perjuicio propio o ajeno.

1.4.2. ¿Qué Necesitamos Saber Sobre El Delito De Estafa Digital?

Doctrinalmente se ha establecido que los elementos esenciales para la configuración del delito son tres: tipicidad, antijuricidad y culpabilidad. En tal sentido, si la conducta realizada por un sujeto es típica, antijurídica y culpable, entonces nos encontraríamos frente a un delito. En estas circunstancias el delito de estafa digital, no está enmarcada en estos presupuestos,

Donde la realidad supera al marco legal, debiendo hacer el juzgador un importante papel interpretativo y el análisis será de tipo informativo.

Los problemas vienen en supuestos donde no está claro que existan todos los elementos; por ejemplo, no siempre es evidente que haya una persona que engaña y otra que es engañada, para ese tipo de casos es cuando debemos remitirnos a la figura de estafa digital que en código penal boliviano no está contemplada como figura jurídica "concepto que no se encuentra contemplado en las leyes nacionales".

El derecho, tiene que adaptarse a la nueva era tecnológica informática. En nuestro país la inexistencia de una legislación penal adecuada, posibilita la comisión de los delitos de estafa digital, dejando al autor de este delito en total impunidad y a la víctima en un estado de total indefensión.

1.4.3. ¿Por Qué Necesitamos Saber Sobre El Delito De Estafa Digital?

Es necesario para poder reglamentar, tipificar, sancionar penalmente este tipo de actos delictivos ya que afecta al patrimonio de las personas naturales y jurídicas y va evolucionando junto con el manejo de tecnologías.

1.4.4. ¿Qué Haremos Para Averiguar Sobre El Delito De Estafa Digital?

Recurrir a la información ya existente sobre delitos de estafa digital efectuados por los autores conocedores del tema; y recurrir a las normas existentes en el ámbito del derecho de los diferentes países, para poder emitir un diagnóstico y poder enfatizar la necesidad de tipificar este tipo de actos delictivos

Por lo cual el presente trabajo de investigación tiene la finalidad de explicar que es el delito de estafa digital, como un delito que no está contemplado en nuestra legislación

1.4.5. Planteamiento Del Problema

¿Cómo encontrar fundamentos jurídicos para proponer la creación de normas complementarias a la legislación Boliviana para darle figura jurídica **al delito de estafa digital,** contra el desplazamiento patrimonial en forma de entrega o simplemente un movimiento contable aparentemente inofensivo, a objeto de evitar el daño económico a las personas naturales y jurídicas, por medio de un complemento normativo en el ordenamiento jurídico del Estado Plurinacional de Bolivia?

El presente análisis desarrolla en forma clara y completa, una guía de investigación jurídica, para proponer medidas en contra de la falta de regulación, en la manipulación informática y uso indebido de datos personas base del cual se genera el delito de estafa digital.

Analizar la práctica de la estafa digital, efectuada con la manipulación de medios digitales, desde la perspectiva sancionadora para encontrar mecanismos jurídicos que regulen y efectivicen la protección a las víctimas, en la ciudad de La Paz

Bolivia con efectos jurídicos de alcance nacional en la en la Red Global Digital" world wide web".

Al encontrarnos **ante Estafas Digitales, mediante la manipulación informática** y uso indebido de datos personales, implica que se susciten **problemas prácticos dentro la estafa digital como:** carding, phishing, pharming, vishing, spamming, falso virus, cartas nigerianas, falsas multas, donaciones fraudulentas, estafa sentimental.

la presente investigación, tiene como objetivo, encontrar mecanismos jurídicos para proporcionar bases jurídicas en el que se pueda tipificar en el código penal, como delitos de orden público, ya que la mayoría de estas interacciones son de carácter privado basado en tratos entre partes con intercambio de información y dinero, y son afectadas el patrimonio de las supuestas víctimas que en su mayoría están dentro de las cifras negras ya que muchos no denuncian haber sido estafados digitalmente.

El problema de este tipo de delitos radica en la gran difusión y comisión de estafas digitales que se realizan en diferentes y variadas formas, sin que estas se lleguen a identificar y sancionar a su debido tiempo por lo que quedan en la impunidad, este mismo hecho hace que el delito de estafa digital sea reiterativo dejando a la persona que es víctima en un total estado de indefensión.

1.5. Delimitación Del Tema Del Trabajo Dirigido

1.5.1. Delimitación Temática

El tema de investigación se enmarca en el ámbito del Derecho público, en el Derecho Penal, y sobre todo en el derecho informático, por tratarse de un tema relacionado con las redes y el uso de instrumentos digitales e informativos que son parte de la comisión de delitos en el derecho penal, por ser una investigación propositiva, para la modificación de la norma, que sea más específica en este tipo de delitos e incorpore en el código penal Boliviano.

1.5.2. Delimitación Espacial.-

La investigación fue realizada en la ciudad de la Paz, pero cuyo efecto abarca a todo el territorio nacional.

1.5.3. Delimitación Temporal.-

La investigación ha definido un periodo de análisis, del ciberdelito de estafa, entre los años 2020 y 2021. En el que coincide con el periodo de la pandemia ya que justamente en este periodo se ha incrementado este tipo de delitos

1.6. Fundamentación E Importancia

La importancia de este análisis de investigación es que el ciberdelito de **Estafa Digital,** ha sido objeto de estudio en los últimos años por lo importante que resulta, el combate contra este tipo de ciberdelitos por la cantidad de dinero que se defrauda debido al contacto con medios digitales. Dichos sistemas se han vuelto populares en comunicación y pago de manera particular el ciberdelito de

estafa digital ha tenido gran demanda por lo que se necesita alcanzar un posicionamiento en contra y combatir el delito de estafa digital, además hay una diversidad de aplicaciones digitales e informáticas populares, como las redes sociales, grupos de telegram, grupos de whatssap, cuyo interés común es divulgar mecanismos para la comisión del delito de estafa.

El presente trabajo de monografía hace referencia a la utilización de instrumentos o plataformas digitales cada vez más populares para la comisión de dichos ciberdelitos.

Dentro de la motivación al trabajo de monografía es que hasta la fecha el ciberdelito de estafa digital se ha incrementado.

Actualmente contamos con muchos artículos y bibliografía que hace referencia a este tipo de delitos informáticos, cabe destacar que cada una de estas referencias consultadas carece de detalles técnicos suficientes para un efectivo combate al ciberdelito de estafa digital.

Hay compañías y falsas empresas que se dedican a la comisión de este delito las cuales presentan marketing y hay que destacar que estos diseños implementados cuentan con originalidad.

1.7. Objetivos Del Tema

1.7.1. Objetivo General.-

Analizar el delito de **estafa digital** como posible figura jurídica capaz de ser incorporada en la legislación penal boliviana identificar sus elementos teóricos investigativos y su regulación actual, sustantiva y procesal,

1.7.2. Objetivos Específicos

1.7.2.1. Objetivo Especifico Teórico

Identificar cuáles son las deficiencias en la legislación boliviana referente al delito de **estafa digital**, si está este tipificado en el código penal boliviano.

1.7.2.2. Objetivo Especifico Práctico

Describir los instrumentos de análisis del delito, para poder brindar un diagnóstico de cómo ha evolucionado, el delito de **estafa digital**, convirtiéndose en un ciberdelito en el ámbito digital.

1.7.2.3. Objetivo Especifico Comparativo.-

Comparar la evolución de regulación ciberdelito con las distintas legislaciones, para proponer una actualización de la norma en el código penal.

1.7.2.4. Objetivo Especifico Desarrollo De La Propuesta

Proponer una actualización de la norma, mecanismos jurídicos, protocolos y manuales, en base al diagnóstico, que englobe una eficaz sanción para plantear una propuesta jurídica efectiva de lucha contra el ciberdelito de estafa digital.

1.8. Métodos Y Técnicas A Utilizarse En El Trabajo

1.8.1. Métodos Generales

1.8.1.1. Métodos De Investigación

La metodología de la investigación utilizada en este trabajo es un diseño metodológico para determinar resultados válidos y fiables que respondan a las metas y objetivos de la investigación. En base a:

1.8.1.2. Método Analítico

Es aquel método de investigación que consiste en la desmembración de un todo descomponiéndose en sus partes o elementos para observar las causas, naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular.

1.8.1.3. Método Sistemático

Significa que no se puede arbitrariamente eliminar pasos, sino que rigurosamente deben seguirse como en el proceso, con el objeto de que no existan vacíos en la manera en que se hace las transferencias patrimoniales.

1.8.2. Métodos Específicos

1.8.2.1. Los métodos cualitativos

Sirven para conocer opiniones, motivos y motivaciones de personas que expresan su opinión personal. Estos métodos ayudan a examinar las razones de la toma de decisiones y a desarrollar hipótesis para posteriores investigaciones cuantitativas, y son muy útiles en las empresas para comprobar el grado de satisfacción de los clientes o los puntos a mejorar.

1.8.2.2. Dogmática Jurídica.-

Conjunto de principios jurídicos de un estatuto, de una constitución o de una ley, es el sentido jurídico del dogma, por eso se habla de la parte dogmática de la constitución, que incluye sus valores y sus postulados, para hacer que las transferencias patrimoniales en medios digitales, sean posibles, sin que por medio se incurra en una estafa digital.

1.8.2.3. Método Deductivo

Es una estrategia de razonamiento empleada para deducir conclusiones lógicas a partir de una serie de premisas o principios

1.8.2.4. Método Inductivo.-

Que se basa en la inducción, para ello, procede a partir de premisas particulares para generar conclusiones generales

Se aplica en el análisis de la información obtenida de fuentes primarias a través de entrevistas realizadas a profesionales abogados y jueces y Policías del área penal, sobre los fundamentos que apoyan o rechazan la incorporación de la falsificación

informática, induciendo las conclusiones a que se lleguen del procesamiento de tales entrevistas siendo así…"partir de lo particular para llegar a lo general."

1.9. Técnicas De Investigación

1.9.1. Técnicas De Investigación Documental

Aquellas que recopilan información acudiendo a fuentes previas, como investigaciones ajenas, libros, información en soportes diversos, y emplea instrumentos definidos según dichas fuentes, añadiendo así conocimiento a lo ya existente sobre su tema de investigación. Es lo que ocurre en una investigación histórica, en la que se acuden a textos de la época.

1.9.2. Técnicas De Investigación De Trabajo De Campo

Aquellas que propician la observación directa del objeto de estudio en su elemento o contexto dado, y que adaptan a ello sus herramientas, que buscan extraer la mayor cantidad de información in situ, o sea, en el lugar mismo. Esto tiene lugar por ejemplo en la investigación estadística, ya que se sale a buscar y clasificar las opiniones de la gente en la calle.

1.9.3. Observación Sistemática

Es un método que permitirá sistematizar las observaciones realizadas en la documentación obtenida acerca de los Delitos Informáticos asimismo se sistematiza la información obtenida tanto en fuentes primarias o secundarias.

1.9.4. Recopilación Documental O Escrita.-

Se utilizará para la obtención de información de fuentes secundarias, con la realización de fichas bibliográficas por tema de la información obtenida en libros, documentos memorias e informes y la revisión de información en documentos publicados, en Internet sobre el tema tratado en los países elegidos con legislación similar a la de nuestro país.

1.9.5. Entrevistas

La entrevista como técnica de investigación, los cual precisan para contrastar la hipótesis," se realizará a dos universos, como a profesionales abogados y jueces del área penal permitiéndonos recopilar información necesaria, para una mejor comprensión de la presente investigación, para lo cual se estructurará una guía cuestionario de preguntas cerradas o abiertas.

1.9.5.1. El Delito de estafa Digital en Bolivia realizada al Sof. Patiño Jefe de la División cibercrimen del departamento de Santa Cruz.

1.- ¿Cuantos casos de estafa digital y en general de delitos informáticos se han podido evidenciar o han llegado a conocimiento de la policía nacional?

Respuesta.- De enero a la fecha, se tiene 66 delitos de estafas, haciendo un total de 07 a 08 casos por mes de conocimiento policial.

2.- ¿En lo referente a ciberdelitos existe alguna unidad en investigación de estafas digitales (carding, phishing, pharming, vishing y spanming)?.

Respuesta.- No existe una unidad especializada de investigación en delitos de estafas digitales como ser carding, phishing, pharming, vishing y spanming, en la legislación Boliviana solo contempla dos artículos “art 363 bis.” (Manipulación informática) y el “art 363 ter” (Alteración, acceso y uso indebido de datos informáticos)

3.- ¿en los delitos de estafa digital cual es el procedimiento que sigue la policía para dar con los autores o autor del hecho?

Respuesta.- Para recepcionar una denuncia de un delito de estafa, lo primero que debe de hacer la víctima es centrar la denuncia que puede ser forma verbal a la policía, de forma escrita a la fiscalía, una vez que se tenga una denuncia se asigna un investigador por la División de **ECONOMICO FINANCIERO** para que luego el investigador realice el informe al fiscal asignado, con los detalles del hecho que se investiga, realizando la petición de los trabajos Técnicos de Investigación, donde intervienen la División de Cibercriminal y las Empresa telefónicas , para que de esta forma dar con el paradero del o de los autores del hecho.

4.- ¿Cómo se coordina con los demás países cuando se evidencia que este es, un delito trans fronterizo?

Respuesta.- A la fecha no se tiene una coordinación directa y legal con los países fronterizos, sin embargo, venimos realizando (ALERTAS CIBERNETICAS) con los países AMERICANOS Y CENTROAMERICANOS Y EUROPEOS, en coordinación con INTERPOL NACIONAL.

5. ¿qué recomendaciones daría a la población para prevenir este tipo de delitos?

Respuesta.- Bueno las recomendaciones son:

- No proporcionar datos personales o médicos por correo electrónico
- No accedas a enlaces o archivos adjuntos provenientes de correos sospechosos, inusuales y/o desconocidos.
- Cambiar la contraseña con regularidad
- No responder a correos y/o mensajes desconocidos
- Evitar instalar software de origen desconocidos

6. ¿de qué manera obstaculiza la labor investigativa el hecho de no tener una jurisdicción especifica al delito de estafa o fraude digital?

Respuesta. Manifestar que los delitos de Cibercrimen y el Narcotráficos son delitos Internacionales que rompen fronteras, por lo que nos vemos en la necesidad de buscar mecanismos de apoyo a los demás Países, para poder mitigar estos delitos que se están incrementado día a día.

7¿Cree Ud. que exista la necesidad de crear una unidad especializada para la investigación de delitos informáticos entre ellos el delito de estafa digital? si la hay, ¿esta cuenta con los recursos técnico forense adecuado?

Respuesta. Si nos vemos, en la necesidad de crear, Unidades Especializadas de investigación en delitos informáticos de estafa digital, manifestar que los países subdesarrollados, están invirtiendo millones de dólares en los ataques cibernéticos, que de una forma u otra nos llega a afectar en el futuro, a la fecha NO contamos con los recursos técnicos forenses adecuados.

1.9.6. Cuestionarios.-

Se efectuó un cuestionario a una población de 68 personas en la ciudad de La Paz Bolivia. Dando resultados expuestos en la monografía, con cinco preguntas las cuales se detalla a continuación

- ¿Sabe usted que es una estafa digital?
- ¿Conoce usted algún caso sobre estafa digital?
- ¿Ha sido usted víctima de estafa digital?
- ¿Realiza Usted compras Online?
- ¿Recibe usted información sobre la estafa digital por parte de su banco o empresa de servicios de internet?
  (Este cuestionario esta realizado en anexos) con su respectivas tabulaciones

2. Capítulo I

2.1. Marco Histórico

2.1.1. Análisis De Los Antecedentes Históricos Del Delito De Estafa Digital

La historia de la estafa es tan antigua como la capacidad de las personas de idear circunstancias en las que pueden sacar el máximo provecho sin siquiera realizar el mínimo esfuerzo o sin desplazarse fuera de su domicilio, poniendo en práctica circunstancias fraudulentas como la que estamos observando en la estafa digital.

La creación de nuevas tecnologías que intermedian en la comunicación entre las personas trae aparejado nuevas posibilidades para su aprovechamiento indebido y aparición de nuevos delitos.

Eso sucedió desde la creación del telégrafo y también posteriormente la incorporación del teléfono a la vida cotidiana de las personas y mucho más aún

con la aparición de la tecnología móvil. Que impulsó a que las personas estén conectadas en la red a tiempo completa.

Con la irrupción de la computadora personal y la posterior expansión de Internet y la World Wide Web; la capacidad de procesamiento de datos e información y el acceso a miles de personas en un medio interactivo de características globales amplió las posibilidades de comisión de hechos ilícitos e ilegales a partir del fácil manejo del surgimiento de entornos digitales “amigables” y aplicaciones prácticas y sencillas en cuanto a su manejo, tanto así como las posibilidades de anonimato en las comunicaciones. Dando un lugar adecuado para cometer estafas digitales a nivel mundial.

El origen de este tipo de delitos informáticos data de la década de los noventa, y su operativa se centraba en el engaño con el objetivo de que una persona pudiera efectuar una transacción patrimonial a cambio de mentiras.

El envío masivo de correos electrónicos fraudulentos a los clientes de entidades financieras (conocido como smishing, o incluso a través de llamadas telefónicas, el denominado vishing), con la finalidad de obtener de éstos los datos y las claves de usuario que les permitirán acceder fraudulentamente a la cuenta de la víctima.

Al principio los mensajes consistían en una burda traducción al español, incluso estaban mal redactados o adolecían de errores ortográficos, pero en la actualidad la técnica se ha ido perfeccionando dotando al mensaje de mayor credibilidad aumentando así las posibilidades de éxito. Incluso la técnica del phishing ha evolucionado migrando hacia otras formas de comunicación online como, en particular, las redes sociales, mediante la colocación de posts en Facebook o Twitter, entre otros, con promociones y beneficios para cuyo disfrute se requiere el ingreso, también en este caso, de información personal y bancaria en las correspondientes webs clonadas.

Otra de las modalidades posibles de obtención de datos y contraseñas del usuario es el caso de phishing a través de malware (acrónimo de "malicious software"), es decir, la implantación de programas denominados maliciosos (entre los cuales, troyanos, virus, gusanos, etc.) en el sistema informático desde el que la víctima maneja sus cuentas bancarias.

2.1.2. Origen y evolución de Internet y los delitos vinculados

No se puede avanzar en el estudio del ciberdelito de estafa digital sin hacer una somera referencia al origen histórico de internet su desarrollo y a sus características técnicas básicas. Es necesario conocer cuáles fueron las razones de su creación y los fines de su existencia, porque muchos de los problemas existentes al investigar un posible delito cometido haciendo uso de internet provienen precisamente de ese origen y de las características sobre las que está configurado.

Parece oportuno hacer una somera mención de las principales etapas por las que ha discurrido la implantación de internet y del modo en que ha ido apareciendo el nuevo elenco de conductas ilícitas vinculadas con la informática y la telemática.

La historia de internet es bastante compleja, por lo que para facilitar el estudio de su evolución y de las conductas delictivas vinculadas a la misma distinguiré cuatro etapas que pueden caracterizarse por los intereses predominantes en cada una de ellas

- la denominada etapa militar, que se corresponde con la década de los años 70 del pasado siglo.
- La denominada etapa académica: años 80 y primeros 90 del siglo XX.
- La denominada etapa comercial: años 90 y posteriores.
- La denominada etapa social: siglo XXI.

2.1.3. La denominada etapa militar.-

Hablar del origen de internet es hablar de DARPA, acrónimo de la expresión en inglés Defense Advanced Research Projects Agency, Agencia del Departamento de Defensa de Estados Unidos, responsable del desarrollo de nuevas tecnologías para uso militar. Esta agencia, denominada originalmente como ARPA, fue fundada en 1958 como consecuencia tecnológica de la llamada Guerra Fría y creó con carácter experimental una red informática llamada ARPANET (Advanced Research Projects Agency Network), que estaba formada por los más prestigiosos centros de investigación académicos y militares del país, con el objetivo de compartir cualquier tipo de información necesaria disponible en cada uno de ellos. Arpanet, antecesora de internet, se creó para conectar varios ordenadores de diferentes centros de investigación en una red. Hasta ese momento todos los sistemas de comunicación existentes eran sistemas punto a punto o extremo a extremo, que solo existía un canal de comunicación entre ambos extremos, y la supervivencia de esos sistemas de comunicaciones dependía de la existencia física del canal. La característica principal de Arpanet es que se desarrollaron e implantaron unos protocolos de comunicaciones que garantizaban la supervivencia de la comunicación en caso de que un enlace o canal fuera destruido en algún siniestro como pudiera ser un terremoto o un ataque nuclear. Para ello, se prescindió de una red centralizada, y se descentralizaron todas las redes conteniendo rutas alternativas y redundantes entre los ordenadores conectados, de tal modo que cada ordenador formaba un nodo en la distribución de la red, ofrecía servicios a otros nodos, o usaba servicios de otros nodos dentro de la red. Nacieron así los protocolos distribuidos que hacían posible que hubiera una comunicación entre dos extremos gracias a la existencia de múltiples caminos para que los mensajes alcanzasen su destino. Eran protocolos que permitían el intercambio de información con independencia de las conexiones físicas de los enlaces de comunicación. Además, cada mensaje era dividido en paquetes y estos paquetes se distribuían y circulaban por los múltiples enlaces y rutas de comunicación. Era en el destino cuando se producía la reordenación de los paquetes entrantes y la confección del mensaje enviado.

En 1969 Arpanet contaba con cuatro ordenadores distribuidos entre distintas universidades del país. Dos años después, ya contaba con unos cuarenta ordenadores conectados, hasta el punto de que el rápido crecimiento de la red hizo que su sistema de comunicación de protocolos distribuidos quedara obsoleto, dando paso al Protocolo TCP/IP, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas.

En esta época inicial se empieza a producir la acumulación de datos de carácter personal de la ciudadanía por parte de los gobiernos, aun cuando no estaba masificado el uso de los ordenadores, y con ello comienzan las preocupaciones en torno al carácter reservado, la acumulación y el uso que podría hacerse de estos datos. Nace así el concepto de “privacy” y del derecho a la misma, que va más allá del tradicional concepto de intimidad y que regula la acumulación en las bases de datos, de carácter informático o no, de información sobre los individuos y el uso que se hace de ella, así como la capacidad de decisión de cada ciudadano respecto a qué datos referentes a su persona deben ser compartidos o públicos

2.1.4. La denominada etapa académica.-

A principios de los años 80 aparecen otras redes similares a Arpanet que pretenden dar cabida a investigadores no integrados en ella.

Se acentuó el carácter académico y de investigación ya que las funciones militares se desligaron de Arpanet y pasaron a MILNET (Military Network o Military Net), una nueva red creada por los Estados Unidos que se integra en la Defense Data Network (1982). La NSF (National Science Foundation) creó en el año 1984 su propia red informática con propósitos científicos y académicos llamada NSFNET (National

Science Foundation Network), que más tarde absorbió a Arpanet. Todas las redes de libre acceso se unieron también a NSFNET, formando el embrión de lo que hoy conocemos como INTERNET.

En 1985 internet ya era una tecnología establecida que se fue globalizando, cuando diversos países, sobre todo europeos, empezaron a conectar sus redes académicas y de investigación a esta infraestructura (España lo hizo en 1990). Además, el incremento de los ordenadores personales trajo consigo el surgimiento de la piratería del software, dando lugar a las primeras infracciones contra la propiedad intelectual.

2.1.5. La denominada etapa comercial.

En 1990 ya deja de existir Arpanet como tal y se sientan las bases de la nueva etapa de internet de marcado carácter comercial que poco a poco va ganando terreno a la vertiente académica, debido a la aparición de aplicaciones revolucionarias como WAIS, Gopher y aún más especialmente la World Wide Web (WWW) o telaraña mundial. En 1993 se produjo la primera versión del navegador "Mosaic", que permitió acceder con mayor facilidad a la WWW, por lo que se abría la red a los legos. A partir de entonces, internet comenzó a crecer más rápido que

otros medios de comunicación,convirtiéndose en lo que hoy todos conocemos: una red que dispone de multitud de servicios o aplicaciones que constituyen las herramientas de trabajo del usuario de internet. El 24 de Octubre de 1995, el Consejo Federal de Redes (Federal Networking Council), responsable de la política de internet en Estados Unidos, aceptó unánimemente una resolución definiendo el término Internet: "El FNC acuerda que la siguiente descripción refleja nuestra definición del término "Internet". Internet hace referencia a un sistema global de información que está relacionado lógicamente por un único espacio de direcciones global basado en el protocolo de internet (IP) o en sus extensiones, es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles con IP, y emplea, provee, o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas aquí descritas". La expansión de internet en la década de los noventa llevó aparejado el surgimiento de un nuevo método para difundir contenidos ilegales o dañosos, tales como pornografía infantil o discursos racistas o xenófobos. Serán precisamente las conductas vinculadas a la difusión de contenidos ilícitos las que más pueden aprovecharse de la enorme implantación que tiene la red a nivel mundial, así como de sus características técnicas que dificultan su descubrimiento, persecución y prueba.

2.1.6. La denominada etapa social.

Paulatinamente se han ido incorporando a internet nuevos protocolos y formas de uso que fomentan la comunicación entre usuarios particulares o grupos de usuarios y la participación en actividades cooperativas. Lo que en general se ha llegado a denominar Web 2.0, con servicios como los diarios personales (blogs), las redes sociales, las enciclopedias colaborativas, el etiquetado social de recursos, etc., que han hecho de internet un medio activo en el que el usuario particular aporta y comparte información y ya no se limita a recibirla19. La facilidad en el acceso y en la búsqueda de información contenida en redes y sistemas informáticos, combinada con las prácticamente ilimitadas posibilidades para su intercambio y difusión ha llevado a un crecimiento explosivo en la cantidad de información accesible siendo significativa la progresiva generalización del uso del correo electrónico y el acceso a través de internet a numerosos sitios o páginas web de distintas partes del mundo. En este período también se consolida la dependencia que los gobiernos y organismos internacionales tienen de los sistemas informáticos, tanto para su buen funcionamiento como para el almacenamiento de datos importantes y/o secretos y ello los pondrá en el punto de mira para la comisión de delitos que atenten contra la seguridad del Estado o para la comisión de ataques terroristas a través de la red. Internet ha generado nuevas oportunidades de enriquecimiento ilícito en forma de estafas y fraudes en las que no sólo intervienen delincuentes individuales sino grupos criminales. Por otro lado, los beneficios obtenidos por las organizaciones criminales les capacitan para acceder a casi cualquier recurso tecnológico, lo cual les sitúa en una posición de ventaja para explotar nuevas oportunidades de negocio y anticiparse a la actuación de las agencias de seguridad, normalmente peor dotadas en ese sentido. Siendo Europa un continente con gran acceso y disponibilidad de internet

por la población, el desarrollo de actividades ilegales y fraudes a través de esta herramienta también se multiplica. En el primer decenio del siglo XXI han predominado nuevos y sofisticados métodos para delinquir, y el uso de tecnologías que dificultan la investigación penal. En definitiva, internet ha cambiado notablemente en su corta existencia, creciendo hasta convertirse en una infraestructura informática ampliamente extendida con capacidad para interconectar a todo el planeta, ignorando fronteras políticas y superando barreras geográficas, lingüísticas, culturales o religiosas, sentando las bases de lo que se conoce como Sociedad de la Información. Consecuentemente, los delincuentes también han hecho uso de las oportunidades que ofrece internet y los delitos cometidos en la red o con ocasión del uso de nuevas tecnologías están en alza dada la rapidez con la que éstas evolucionan. El interrogante ante tal evolución es cómo hacer frente a esta nueva actividad criminal, lo que supone un auténtico desafío en el que están implicados todos los poderes del Estado.

Esos progresos han tenido también su reflejo en la delincuencia y criminalidad. Han aparecido nuevos tipos de delitos, así como nuevas modalidades y peculiaridades en la comisión de los clásicos delitos. Más aún, las consecuencias de la conducta criminal pueden ser de mayor entidad y trascendencia puesto que no están restringidas por limitaciones geográficas o fronteras nacionales. La propagación mundial de virus informáticos, como por ejemplo el virus "I love you" por un estudiante desde Las Filipinas afectando a miles de equipos y sistemas informáticos, proporcionó una prueba de esta realidad.

3. Capitulo II

3.1. Marco Conceptual - Definiciones

Carding.- falsificar y copiar tarjetas bancarias o robar información financiera de las tarjetas de crédito o débito, o también de datos personales que se hayan proporcionado online.

Phishing.- es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito

Pharming.- es un tipo de ciberataque con el que se intenta redirigir el tráfico web al sitio del atacante, explotando vulnerabilidades de software en los sistemas de nombre de dominio (DNS, por sus siglas en inglés) o en los equipos de los propios usuarios, que permiten a atacantes redirigir un nombre de dominio a otra máquina distinta.

vishing.- un tipo de ataque peligrosamente eficaz que se apoya en técnicas de ingeniería social y en el cual el atacante se comunica telefónicamente o vía mensaje de voz haciéndose pasar por una empresa o entidad confiable con la intención de engañar a la víctima y convencerla de que realice una acción que va en contra de sus intereses.

Spamming.- El término SPAM o mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo),

habitualmente con contenido publicitario y que generalmente son enviados de forma masiva perjudicando al receptor de dicho mensaje.

Falso virus.- son mensajes que circulan por e-mail que advierten sobre algún virus inexistente.

Cartas nigerianas.- Una estafa por pagos y honorarios anticipados, en el que la víctima está convencida de adelantar dinero a un extraño. la víctima debe esperar que se le devuelva una suma de dinero mucho mayor. La víctima, por supuesto, nunca recibe nada de este dinero.

Falsas multas.- Los estafadores mandan correos electrónicos masivos utilizando el logo y la imagen del organismo, en este caso la Dirección General de Tránsito, y a través de un enlace que descarga programas maliciosos en nuestro ordenador pueden acceder a datos bancarios o personales. en el mensaje avisan de una supuesta multa a los conductores.

Donaciones fraudulentas.- Mientras cada día aumenta el número de casos positivos de COVID19, también aumentan los casos de estafadores que se aprovechan de la emergencia sanitaria que acontece en todo el mundo.

Una campaña fraudulenta que utiliza servicios de mensajería y redes sociales para difundir una falsa campaña de donación para combatir el coronavirus.

Estafas sentimentales.- Millones de personas recurren a aplicaciones de citas en línea o sitios de redes sociales para conocer a alguien. Pero en lugar de encontrar el amor, muchos encuentran a un estafador que intenta engañarlos para que envíen dinero.

Backup: copia de seguridad.(Steven Nelson • 2011 Pro Data Backup and Recovery - Página 186)

Blog: página en internet que se actualiza de forma periódica para la expresión de pensamientos u opiniones que suele adoptar el formato de un diario personal (Eva Sanagustín Fernández • 2009 Tu blog paso a paso: manual para iniciarse en el blogging - Página 22)

Buscador: es una herramienta que permite buscar páginas en internet referidas a un tema específico o relacionado con ciertas palabras clave.

Cliente/Servidor (Client/Server): el modelo cliente-servidor es el sistema de organización de las conexiones entre ordenadores que se utiliza en internet, y en general en todas las redes de ordenadores. Se basa en la clasificación de los ordenadores de la red en dos categorías: las que actúan como servidores (oferentes de información) y otras que actúan como clientes (receptores de información). (Juan Carlos Moreno Perez Sistemas informáticos y redes locales)

Cloud: la “nube” es una metáfora empleada para hacer referencia a determinados servicios que se utilizan a través de internet, que facilita la utilización de recursos

desde un lugar remoto.(Ainoa, Celaya Luna • 2017 Cloud: Herramientas para Trabajar en la Nube)

Correo no deseado o SPAM: correo que no es solicitado y que suele tener un remitente desconocido con la finalidad de promover una página web o un determinado producto. (MIGUEL, SÁNCHEZ ESTELLA, ÓSCAR • 2011 Sistema Operativo, Búsqueda de la Información)

Dirección IP: es un número identificativo y único de cada dispositivo que se conecta a internet. (José Luis Rodríguez Laínz • 2010 Dirección IP, IMSI e intervención judicial de comunicaciones…)

DNS (Domain Name System/Server, servidor de nombres de dominios): sistema de ordenadores que se encarga de convertir las direcciones electrónicas de internet (como http://www.mde.es) en la dirección IP correspondiente y viceversa. Componen la base del funcionamiento de las direcciones electrónicas en Internet. El sistema DNS está organizado jerárquicamente. Por ejemplo, en España, la gestión de todos los nombres de dominio bajo el dominio de primer nivel ".es" corresponde a la Entidad Pública Empresarial Red.es dependiente del Ministerio de Industria. (Joaquín Andreu • 2011 Servicios DNS Servicios en red)

Dominio: Es un término empleado en el mundo de internet para referirse al nombre que sirve para identificar direcciones de computadoras conectadas a internet. (Por ejemplo: www.google.es). (Juanjo Boté • 2013 Aprende HTML efectivo: Conceptos básicos para crear páginas web

HASH: Los hash o funciones "resumen" son algoritmos matemáticos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos). La palabra hash hace referencia a la función que se emplea, aunque por extensión también se utiliza para designar el resultado que se obtiene al aplicar la función. Por definición no pueden existir dos archivos distintos que tengan el mismo hash y además dos archivos que sólo se diferencien en un bit tendrán hashes totalmente distintos. La función hash se utiliza para: identificar inequívocamente un archivo (es como el ADN de ese archivo), asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento. (Rick Miller, Raffi Kasparian • 2006 Java for Artists: The Art, Philosophy, and Science of ... - Página 706)

IMSI: acrónimo de International Mobile Subscriber Identity (Identidad Internacional del Abonado a un Móvil). Es un código de identificación único para cada dispositivo de telefonía móvil, integrada en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS (3 G). Este número de abonado conforme a la norma internacional ITU E.212, está compuesto por el MCC o código del País (3 dígitos), por ejemplo, 214, que correspondería a España; por el

MNC o Código de la red móvil (2 ó 3 dígitos), por ejemplo, 07, que correspondería a la operadora MOVISTAR; y finalmente por el MSIN (número de 10 dígitos) que contiene la identificación de la estación móvil.(Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen • 2005 UMTS Networks: Architecture, Mobility and Services - Página 155)

IMEI: del inglés International Mobile Equipment Identity (Identidad Internacional de Equipo Móvil) es un código pregrabado en los teléfonos móviles GSM/UMTS que identifica al aparato unívocamente a nivel mundial, y es transmitido por el aparato a la red al conectarse a ésta. Esto quiere decir, entre otras cosas, que la operadora que usemos no sólo conoce quién y desde dónde hace la llamada (SIM) sino también desde qué terminal telefónico la hizo. La empresa operadora puede usar el IMEI para verificar el estado del aparato mediante una base de datos denominada EIR (Equipment Identity Register). Se puede conocer tecleando "asterisco, almoadilla, 06, almohadilla". (Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen • 2005 UMTS Networks: Architecture, Mobility and Services - Página 158)

Ingeniería Social: es el proceso de manipular a usuarios legítimos para obtener información confidencial, con el objetivo de divulgar información, cometer fraude u obtener acceso a un sistema informático. Son técnicas basadas en engaños que se emplean para dirigir/controlar la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en determinados enlaces, introducir contraseñas, visitar páginas webs, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social. En el caso de las redes sociales, los atacantes disponen de una gran cantidad de información 26 tan sólo con ver el perfil de su víctima (sexo, fecha de nacimiento, aficiones, formación, carrera profesional, etc.) lo que favorece el despliegue y empleo de estas técnicas.(Carlos a Barbero Muñoz, Antonio Angel Ramos Varon • 2020 Throughout this book, all kinds of techniques, physical and logical, to perpetrate attacks based on Social Engineering will be described: phishing, obtaining information through open sources (OSINT), techniques of manipulation of people, Conoce todo sobre Hacking con Ingeniería Social. Técnicas).

Internet: en forma muy resumida, es una red de ordenadores o equipos informáticos que se comunican entre sí empleando un lenguaje común conocido como conjunto de protocolos TCP/IP. Contrario a la creencia popular, WWW no es un sinónimo de internet, es un servicio que es parte de internet. (Raquel González Sabín • 2005 Nuevas Tecnologías Aplicadas a La Gestión De RR.HH.)

Login: proceso de seguridad que exige que un usuario se identifique con un nombre (user-ID) y una clave, para poder acceder a una computadora o a un recurso. (Ying Bai • 2021 Oracle Database Programming with Visual Basic.NET: Concepts)

Malware: es un término general que se le da a todo aquel software que tiene como propósito explícito infiltrarse o dañar a la computadora. (Cameron H.

Malin, Eoghan Casey, James M. Aquilina • 2008 Malware Forensics: Investigating and Analyzing Malicious Code)

Navegador (Browser/Web Browser): es un programa que permite ver páginas de internet. Específicamente traduce documentos escritos en HTML a contenido visible por personas. (Ana Belén García Mariscal • 2015 UF2405 - Modelo de programación web y bases de datos - Página 457)

Nickname (Nick, sobrenombre o alias): nombre figurado que un usuario de internet utiliza, por ejemplo, para participar de un chat. (Patrick Lorenz • 2008 ASP.NET 2.0 Revealed - Página 363)

Phishing: término empleado en el mundo de internet para referirse a un engaño o estafa diseñada para obtener información confidencial, como lo son números de tarjetas de crédito, claves de acceso, datos de cuentas bancarias u otros datos personales.(Luis Fernando Rey Huidobro • 2012 La estafa informática: relevancia penal del phishing)

Redes sociales: son plataformas Web compuestas por grupos de personas que forman una comunidad, y que a través de internet y de distintas herramientas interactivas, pueden relacionarse, comunicarse y compartir contenidos con otros miembros de esa misma comunidad o grupo, de un modo público o semipúblico, en función de las distintas posibilidades de asociación o acceso a la red y de los intereses, propiedades u objetivos comunes de dichos usuarios. Desde un punto de vista general, la primera gran división a la hora de clasificar las redes sociales es en función de si se necesita o no un perfil para acceder a ella. En base a este criterio, las redes se clasificarían en: a) Redes sociales directas: es necesaria la creación de un perfil por cada uno de los usuarios. Entre ellas cabría una segunda división atendiendo a:

La finalidad: de ocio (Facebook, Tuenti, YouTube, Twitter), uso profesional (Facebook, Twitter, LinkedIn). - El modo de funcionamiento: de contenidos (YouTube), basada en perfiles personales o profesionales (Facebook, LindekIn…), microblogging (Twitter) - El grado de apertura: públicas (Facebook, Tuenti, YouTube…) o privadas (Yammer).

El nivel de integración: vertical (acotado a un grupo de usuarios a los que les une una misma formación, interés o profesión (Dir&Ge) u horizontal (Youtube, Twitter, LindekIn). b) Redes sociales indirectas: no es necesario la creación de un perfil. En este caso un usuario propone un tema y los demás pueden comentar o participar de esa aportación. En este apartado contaremos con Foros y Blogs.(Kadushin, Charles • 2013 Comprender las redes sociales: Teorías, conceptos y hallazgos)

Router: Es un hardware que funciona a modo de semáforo para controlar el flujo de datos que se transmiten entre redes de ordenadores. Determina qué debe ir y a dónde. Es el encargado de guiar los paquetes de información que viajan por internet hacia su destino. (Iván Skowronski • 2020 Trucos para tu Router Wi-Fi)

Spyware: es un programa que se instala en el ordenador, usualmente con el propósito de recopilar y enviar información, que puede ser desde las costumbres de navegación en internet hasta números de tarjetas de crédito, claves de acceso, etc. (Goncalo Paxe Jorge Miguel 2019 PROTEGE TU PC CONTRA SPYWARE Y ADWARE: La guía definitiva ...

Troyano: es un malware destructivo que se disfraza de un programa benigno. Se diferencian de los virus en que los troyanos no se replican a sí mismos, aunque son igualmente peligrosos y destructivos. (Cristian Barría Huidobro, Sergio Rosales Guerrero • 2021 Amenazados: Seguridad e inseguridad en la web)

URI y URL: URI son las siglas en inglés de Uniform Resource Identifier y sirve para identificar recursos en Internet. URL son las siglas en inglés de Uniform Resource Locator y sirve para nombrar recursos en internet.(D. Miguel Ángel Guevara Jiménez, 2014 Sistema operativo, búsqueda de la información)

Wi-Fi: es una marca registrada que también se usa como el término utilizado para nombrar la tecnología con la que se conectan diversos dispositivos electrónicos de forma inalámbrica. (Gloria Areitio y Ana Areitio Información, Informática e Internet: del ordenador personal)

Software: Se refiere a (i) programas de computadora que comprenden una serie de instrucciones, reglas, rutinas o declaraciones, independientemente del medio en el que se grabe, que permiten o hacen que una computadora realice una operación o serie de operaciones específicas; y (ii) información registrada que comprende listados de código fuente, detalles de diseño, algoritmos, procesos, diagramas de flujo, fórmulas y material relacionado que permitiría producir, crear o compilar el programa de computadora. El software no incluye bases de datos informáticas ni documentación de software informático.

Código desarrollado a medida: el código desarrollado a medida es un código que se produce por primera vez en el cumplimiento de un contrato federal o que está totalmente financiado por el gobierno federal, incluido el código, o partes segregables del código, para las cuales el gobierno podría obtener derechos ilimitados bajo Regulaciones Federales de Adquisiciones (FAR) Pt. 27 y suplementos FAR de la agencia pertinente. El código desarrollado a medida también incluye código desarrollado por empleados de la agencia como parte de sus funciones oficiales. A los efectos de esta política, el código desarrollado a medida puede incluir, entre otros, código escrito para proyectos de software, módulos, complementos, scripts, middleware y API; Sin embargo, no incluye código que sea verdaderamente exploratorio o de naturaleza desechable, como el escrito por un desarrollador que experimenta con un nuevo lenguaje o biblioteca.

Software de código mixto: una solución de software de código mixto incorpora tanto código de código abierto como propietario.

Software de código abierto (OSS): software al que puede acceder, usar, modificar y compartir cualquier persona. OSS a menudo se distribuye bajo

licencias que cumplen con la definición de "Código Abierto" proporcionada por la Iniciativa de Código Abierto Plurinacional de Bolivia **CREANDO LA INFRAESTRUCTURA INFORMATICA PLURINACIONAL DE BOLIVIA** y / o que cumplen con la definición de "Software Libre" proporcionada por el Software Libre. Fundación.

Software propietario: software con derechos de propiedad intelectual que son retenidos exclusivamente por un titular de derechos (por ejemplo, un individuo o una empresa).

Código fuente: comandos de computadora escritos en un lenguaje de programación de computadoras que deben ser leídos por personas. Generalmente, el código fuente es una representación de nivel superior de los comandos de computadora tal como los escriben las personas y, por lo tanto, debe ensamblarse, interpretarse o compilarse antes de que una computadora pueda ejecutar el código como un programa.

4. Capitulo III

4.1. Marco teórico.-

4.1.1. Antecedente histórico.-

1903 Carlo Ponzi un migrante italiano que paso a la historia como el creador de la mayor estafa piramidal financiera en la historia, habían sido tentados por las mágicas palabras que se repetían como un eco, “todo es posible en EEUU” llegue a EE.UU. con 2 dólares y 50 centavos en efectivo y 1 millón de esperanza y esas esperanzas nunca me abandonaron, (Carlo Ponzi- Wikipedia enciclopedia libre).

Las estafas digitales en un comienzo nacieron con la misma forma de una estafa piramidal pero unido al internet este delito creció exponencialmente al llegar a un gran número de personas con la promesa de recibir cuantiosas ganancias en el menor tiempo posible.

Actualmente, La Estafa Digital engloba una serie de actividades con diversa variedad de conductas encaminadas a llevar al engaño a la víctima utilizando medios digitales, para que posteriormente el estafador pueda beneficiarse patrimonialmente, causando un perjuicio al sujeto pasivo que en su generalidad es necesitado económicamente, por falta de trabajo o condiciones económicas desfavorables en su entorno social las personas están pasando momentos difíciles, en que mucha gente se aprovecha de ello.

Este tipo de delitos se ha visto proliferar en la red, potenciadas con el auge de las nuevas tecnologías, principalmente las relacionadas con Internet por su fácil difusión en donde prolifera un marketing en base a un modelo de negocio, prometiendo ganancias hasta del 50% de la inversión en corto plazo.

En cuanto a la estafa digital, es de destacar que la nueva figura jurídica pretende proteger el patrimonio de los ataques que propician las nuevas tecnologías.

El lugar donde se encuentra el estafador desde el que lanza sus campañas de captación, es diferente al lugar donde la víctima recibe el ataque que puede o no coincidir con el domicilio de su cuenta bancaria, recibiendo y extrayendo la suma defraudada que es enviada por él estafador digital que generalmente es enviada al extranjero

Un acto de disposición económica en perjuicio de tercero que se concreta en una transferencia no consentida.

4.1.2. Introducción.-

La presente investigación del delito de **Estafa Digital** por medios informáticos, muestra la gran complejidad de manejo jurídico de este tipo de delitos con sus diferentes variantes, resaltando el hecho de que, la inteligencia artificial, ha ocupado el lugar de los sujetos activos del delito (personas), poniéndolos en el anonimato, haciendo imposible la identificación del delincuente, La inteligencia Artificial son programas que interactúan entre el hombre y la computadora, dando a los delincuentes un instrumento valioso para poder lograr su objetivos delictivos siendo anónimos en tal circunstancia , las computadoras utilizan Bots, (programas que simulan ser personas o entidades o instituciones) y los chatbots (Los chatbots, bots de charla o bots conversacionales, son programas informáticos basados en inteligencia artificial (IA) diseñados para simular conversaciones con personas mediante respuestas automáticas).

4.1.3. Internet y el cambio en la concepción tradicional del delito.

Una vez vistas las características técnicas básicas que presenta internet, procede tratar ahora en qué medida esas características son particularmente relevantes a la hora de facilitar la comisión del delito , para analizar a continuación los problemas y retos que plantea la aparición de los nuevos tipos penales de la sociedad de la información. Tal como ha quedado dicho, internet es una red mundial con conexiones instantáneas y con una estructura descentralizada que se basa en la representación digital de la información y que permite las conexiones en tiempo real entre las personas independientemente de su ubicación. Ello ofrece oportunidades especiales para cometer delitos, pues el tiempo, la distancia y las fronteras nacionales son mucho menos importantes que en los delitos tradicionales. Pues bien, todas estas características relacionadas entre sí representan las peculiaridades que favorecen la comisión de ciertos delitos lo que dificulta al mismo tiempo su investigación y persecución judicial, a saber

4.1.4. El desarrollo de internet ha tenido su reflejo en la delincuencia y la criminalidad,

Han aparecido nuevos tipos delictivos, así como nuevas modalidades en la comisión de delitos tradicionales. Actualmente lo informático se constituye no sólo en un medio sino incluso en un objeto potencial para la realización de ilícitos estrictamente telemáticos o cibernéticos

4.1.5. Internet es una red mundial

Que presenta un alcance global a la que se puede acceder desde cualquier parte del mundo prácticamente al instante. Ello permite que los potenciales delincuentes puedan actuar desde cualquier lugar del mundo, buscar a las víctimas más vulnerables en cualquier lugar y efectuar los ataques también en y desde cualquier lugar, evitando la persecución gracias a la deslocalización que ofrecen este tipo de actividades cibernéticas. Internet y su desarrollo global no sólo ha acrecentado su significación criminológica, sino que ha dificultado en mayor grado la posibilidad de acreditación del hecho punible, de las personas responsables, e incluso del equipo origen de la acción ilícita.

4.1.6. Este alcance global conduce a la desterritorialización,

Lo que implica que el fenómeno de la ciberdelincuencia sea casi por definición, internacional. Ello conlleva dificultad en la persecución de los delitos con los consiguientes desafíos legales de la cooperación internacional para perseguir un ilícito de estas características. Piénsese, por ejemplo, que un sujeto puede cometer un delito contra otro situado a miles de kilómetros del primero, mientas que la información está en otro lugar diferente de éstos. Se ha acrecentado la característica transnacional o transfronteriza de estos delitos, con los consiguientes problemas competenciales entre jurisdicciones de distintos Estados, la disparidad de sus normativas penales en la sanción de una misma conducta, o incluso su consideración o no como delito y la existencia de los llamados “paraísos informáticos”, auténticos reinos de impunidad para el delincuente por internet. La situación puede llegar a producir una verdadera impunidad, si no se articulan los remedios adecuados.

4.1.7. El gran número de usuarios

Las frecuencias de acceso y uso, así como la libre circulación y navegación tanto para emitir, trasferir y difundir información como para acceder a ella por medio de la red, permiten que los cibernautas puedan ser al mismo tiempo potenciales víctimas como perpetradores de los hechos ilícitos.

4.1.8. Facilita el anonimato

Tanto para los delincuentes con conocimientos técnicos que pueden recurrir a la utilización de herramientas para la navegación anónima, como también para aquellos que carecen de esos conocimientos técnicos, pues les otorga cierto y relativo anonimato cuando operan a gran distancia detrás de un número IP, dirección de correo electrónico o perfil, ya que a menudo no es fácil rastrear a un individuo específico. Aunque pudiera seguirse el rastro digital dejado al iniciar la comunicación y proseguir la navegación y accesos correspondientes, hasta conocer desde qué terminal y a través de qué servidor se operó en la red, no es tan fácil identificar el individuo concreto que realmente lo perpetró.

4.1.9. Permite la interacción distante con las víctimas

Eliminando posibles barreras sociales que los delincuentes encuentran en la interacción de persona a persona. La ciberdelincuencia implica por lo tanto “las relaciones anónimas entre perpetradores y víctimas”.

4.1.10. Las propias características físicas Técnicas y lógicas

Facilitan la manipulabilidad de datos y el software con un costo mínimo, ya que se basa en la representación digital (lo que permite la copia sin pérdida de calidad, y la alteración sin huellas visibles). De este modo, puede conseguirse el acceso a ficheros y archivos de muy variada naturaleza y trascendencia sin autorización de sus titulares, la manipulación de sus contenidos por diversos procedimientos, incluida la alteración del software conforme a las necesidades o propósitos del intruso. Así, se afirma que "lo real puede convertirse en falso, el original en copia y el ser en identidad virtual”.

4.1.11. Permite la automatización en la comisión del delito

En aquellos casos en los que un virus es lanzado a internet puede replicar y atacar a millones de ordenadores al mismo tiempo, pero también a lo largo de períodos de tiempo, e incluso personalizarse para crear un nuevo virus.

4.1.12. Puede generar un daño de mayor escala

De mayor consideración (por ejemplo, cuando una fotografía es publicada en la red adquiere un alcance global y un impacto mucho mayor que por cualquier otro medio).

4.1.13. Puede atacar a diversas víctimas pero ocasionar a cada una de ellas un daño muy pequeño

(Como por ejemplo, a través de las técnicas por las cuales se sustrae 0,5 céntimos de euro de diez mil cuentas bancarias diferentes mil veces). Este problema de mínimos puede ser uno de los mayores retos de la ciber delincuencia ya que reduce los incentivos para informar, investigar y enjuiciar el delito

4.1.14. Facilita o magnifica la comisión de delitos

cuyo injusto viene fundamentado en los contenidos de la información, como son los casos de apología del terrorismo, la discriminación de determinados grupos de personas, la xenofobia, la comisión de injurias contra terceros, la difusión de pornografía infantil, la distribución e intercambio no autorizado de obras de creación intelectual etc… Internet no solo facilita la difusión por sus características, sino también debido a que abarata los costes de difusión al tiempo que favorece la comunicación y el intercambio entre personas afines (ej. pornografía infantil).

4.1.15. Internet facilita el comercio de la información que se ha convertido en un activo valioso tanto en el mercado legal

(Música, películas, software, libros) como en el mercado negro, donde los números de tarjetas de crédito, información personal y contraseñas se

comercializan para facilitar el fraude y el robo. Incluso se ha convertido internet en un medio a través del cual se realizan acciones de ciberguerra y ciberespionaje

4.1.16. La estructura descentralizada y no jerarquizada de la red

Es incompatible con la existencia de órganos o instituciones que controlen la cantidad información que circula en la red lo que imposibilita o dificulta filtrar, supervisar o controlar dicho volumen de información.

4.1.17. Su innovación constante permite nuevas técnicas y herramientas

Que se desarrollarán con el objetivo de burlar las medidas de seguridad existentes y cometer nuevos delitos.

4.1.18. Desde el punto de vista de la prueba

Se dificulta su obtención por el carácter intangible de los datos y de la información que contienen y por el carácter eminentemente volátil al estar en un espacio virtual y en un sistema de continua transferencia y transmisión que permite su supresión, alteración, transformación u ocultación en cualquier momento. También porque presenta serias dificultades para lograr la conservación o almacenamiento de los datos en un soporte. Y porque aún en este caso, la falta de visualización de los datos almacenados electromagnéticamente dificulta de forma considerable la acreditación del ilícito, pues cualquiera que quisiera comprobarlos y revisarlos no puede hacerlo directamente sobre los datos, sino que siempre debe acudir a los términos del ordenador y a las comunicaciones a través de la pantalla, que además, pueden haber sido objeto de manipulación. Aunque los autores tienden a señalar estos factores de riesgo como las principales causas a tener en cuenta, por lo general, existe acuerdo en que es su combinación lo que hace que la ciberdelincuencia sea un reto especial que produce cambios en la delincuencia ordinaria. En definitiva, el Derecho penal se enfrenta a una criminalidad progresivamente más peligrosa a la que el derecho procesal debe dar también la respuesta necesaria.

4.1.19. Estafa Digital.-

Es sinónimo de fraude, es un delito contra la propiedad o el patrimonio, utilizando recursos digitales con el fin de obtener cuentas bancarias con o sin efectivo para respaldar operaciones mercantiles o crear préstamos suplantando la identidad de las personas a nivel internacional.

El núcleo del tipo penal de estafa digital consiste en el **engaño**. El sujeto activo del delito se hace entregar un bien patrimonial, por medio del engaño; es decir, haciendo creer la existencia de algo que en realidad no existe. Por ejemplo: se solicita la entrega de un anticipo de 500 dólares como entrada para la adquisición de bitcoin, con una promesa falsa de ganar intereses sobre su inversión, cosa que después de un determinado tiempo dicha inversión no existe o es privatizada por el bróker (o la persona encargada de realizar dicha inversión) cuya característica es anónima.

4.1.20. ¿Cómo identificar una estafa Digital?

1.- para ganar dinero tienes que poner dinero

2.- te ofrecen una oportunidad de negocio de ganancia rápida de dinero

3.- no se vende un producto y no se vende un servicio

4.- no necesitas hacer mucho esfuerzo

5.- tienes que reclutar personas y no hacer ventas

6.- no ofrece factura, no tiene una marca registrada y no tiene negocio legal.

7.- vincula con modelos conocidos como network marketing, marketing de afiliado o marketing digital

8.- tienen que tener un sitio web detallado, explicando quien es con quien trabajo, experiencia y lo que han logrado.

9.- opciones para reclamar si se siente engañado, opciones de devolución o de dinero

4.1.21. Agencias de marketing de estafas digitales.-

El marketing digital es, a día de hoy, una industria que genera miles de millones de dólares y euros anualmente. Por ello, no es de extrañar que los anunciantes inviertan en ella cantidades desorbitantes de dinero, cada vez más elevada, con el fin de incrementar sus ingresos. Según un estudio realizado por la World Federation of Advertisers, esta cifra ascendió a los 130. 000 millones de euros en 2016. En España, la inversión total en publicidad digital en 2017 fue de 754 millones de euros, lo que supone un incremento del 24% en comparación a los 606 millones del año 2016 (IAB, 2017).

Sin embargo, no es oro todo lo que reluce. Este mercado multimillonario es también objeto de un fraude que crece a un ritmo desenfrenado.

La agencia The & Partnership cifró las pérdidas ocasionadas por este delito en 16. 400 millones de dólares en 2017 (unos 13 500 millones de euros), cuatro millones más que en 2016, y es probable que estás cantidades aumenten en los próximos años. La WFA estima que el fraude producirá unas perdidas 150 000 millones de dólares (124 000 millones de euros) para los anunciantes en 2025. Estas cifras convierten al fraude publicitario en la actividad ilegal más lucrativa del mundo después del tráfico de drogas.

Poco a poco, las empresas anunciantes comienzan a darse cuenta de primera mano de las consecuencias que ello acarrea en sus inversiones en marketing digital. Una encuesta realizada por el Collectif de la Performance & l'Aquisition (CPA) en Francia confirma esta tendencia. El 60% de los anunciantes eran conscientes de que al menos un 10% del presupuesto invertido sería objeto de acciones fraudulentas. No obstante, sólo el 23% imponen a sus partners de display implementar soluciones técnicas para luchar contra el fraude.

Conozcamos los diferentes tipos de fraude digital. Existen muchos, pero es posible agruparlos en cinco grandes categorías:

4.1.22. La venta de espacios ficticios digitales

Conocidos como espacios publicitarios “fantasma” creados con el objeto de hacer creer a los ad-servers que una publicidad se ha insertado correctamente. Se identifican distintos tipos de espacios ficticios, como el pixel stuffing, el Ad Stacking, el autorefresh…

Y es que la mayoría de PYMES y autónomos no saben qué es el marketing o qué servicios presta una agencia de marketing online, por lo que a estas personas les resulta bastante sencillo prometer el cielo a cambio de muy poco.

4.1.23. La venta de audiencias ficticias digitales: granjas de clics

Éstas pueden estar formadas por dos tipos de perfiles: en primer lugar, el tráfico humano fraudulento, que suele ser el resultado de que los editores compren tráfico para su sitio. Muchos esquemas de «trabajo desde casa» implican contratar personas para interactuar en los sitios que compran tráfico. Por lo tanto, parece que su anuncio recibe muchos clics y esos clics incluso se registran y se convierten en clientes potenciales, pero en realidad nunca se convertirán. Dentro de este contexto encontramos también las “granjas de clics”, que afectan especialmente a la publicidad y al marketing digital en las redes sociales.

En segundo lugar encontramos aquellas audiencias formadas por robots malintencionados que tienen como objetivo crear un público ficticio y simular el comportamiento humano con el fin de generar visitas a los sitios web, impresiones o clics en los anuncios, etc. Existen diversos tipos de fraude con bots, como el “relleno de cookies”, los “bots independientes”, los “centros de datos bot”, etc. Aunque antes eran fáciles de interceptar, cada vez simulan mejor el comportamiento humano. Esto hace que sea una de las formas más utilizadas de cometer fraude.

4.1.24. La venta de segmentos ficticios digitales

Este tipo de fraude sucede cuando los criterios de segmentación no son respetados, voluntariamente o no, por los partners (agencias, editores, proveedores de datos de terceros…). Es lo que se conoce como alteración de la segmentación. Para el anunciante, esta práctica implica un gasto de medios que no corresponde a su resumen inicial, lo que puede afectar al rendimiento de su campaña de marketing digital.

4.1.25. La venta de resultados ficticios digitales

Es lo que se conoce como “robo de la conversión” mediante la manipulación de la solución de tracking. La manera más fácil de asegurar un buen rendimiento es asegurarse de que las cifras muestren la verdad correcta. Existen estafas de diversos tipos:

- Alteración del tracking (fuente UTM).

- Softwares adicionales que se pueden agregar a un navegador.
- Retargeting enmascarado como targeting.
- El tráfico incentivado y desorientado.

Estos son, a grandes rasgos, los diferentes tipos de fraude digital. Desde la experiencia de Eulerian Technologies con nuestra plataforma, podemos destacar que una analítica detallada con una granularidad de datos extrema y sin muestreo va a proporcionar un control absoluto de todos los puntos de contacto entre usuarios y marca. De esta manera es posible determinar la contribución real de los diferentes canales y socios de marketing con los que se trabaje, lo que ayuda a prevenir e identificar más fácilmente cualquier tipo de fraude al que nos enfrentemos. Y recordemos: nadie está a salvo del fraude en la publicidad digital. ¡Mantengámonos atentos! Fuente: Pierre Saisset, director general de Eulerian Technologies para España.

4.1.26. ¿Cuáles son los tipos de fraude más habituales a los que se enfrentan los profesionales del Marketing y la publicidad online?

Recurrencia del fraude en los problemas del marketing y publicidad digital, fuente de ingresos económicos, hay practicas cuestionables dentro de la industria la publicidad digital, existen datos que afirman que la estafa digital está bastante extendido, y las empresas poseedoras de marcas se han cruzado de forma habitual con este tipo de fraude,

Según estudios por whiteops y Renegade, realizo encuestas a más de un centenar de líderes en marketing digital, la mayoría de las empresas que requieren este tipo de servicio han visto fraude.

El fraude más habitual, es el fraude en la compra de medios

Bots, que hacen clic en los anuncios, 23% con bots, los bots hacen clic en anuncios. Para robo de dinero

Generación leads.- cubren formularios con información falsa o robada, para robar el dinero

Retargering.- aplicación de compras por medio de personas fictas (bots) con promesas de venta a mayor cantidad de personas, juegan con el sistema para sacar dinero,

Abuso de programas inventivos.- por bots que juegan con el sistema para sacar beneficio económico, (bots que apuestan en plataformas fictas) incluyen cualquier tipo de apuesta de grandes sumas de dinero. En equipos de futbol, de básquet, de futbol americano, de raquet, rugby, de hookey, en todo lo que se pueda apostar, hundiendo en la miseria a todos los equipos que llegan a participar de dicha apuesta)

4.2. Como prevenir ser víctima de estafa Digital

4.2.1. Gestionar una Auditoría De Marketing Digital Inicial

Cualquier agencia que trabaje bien, el primer paso que dará será la realización de una auditoría e investigación de mercado. Si no te la han planteado, exígeles una. Este informe inicial es muy importante para poder valorar el trabajo que se va a desarrollar; de otra forma el presupuesto no se adaptaría a la realidad.

Si no te van a realizar la auditoría de marketing, querrá decir que el "trabajo" que van a realizar no será de calidad.

4.2.2. Exigir Experiencia Demostrable – Los Casos De Éxito

Lo mejor para saber si la agencia digital que estás contratando es una estafa o no, es pedirles referencias y una experiencia demostrable.

Quizá no te puedan dar detalles precisos, pero sí que te pueden hacer un planteamiento de logros que hayan obtenido anteriormente. Nosotros te animamos a que les hagas preguntas sobre otros casos de éxito en los que hayan trabajado, ofreciendo un servicio similar al que tú vas a contratar.

4.2.3. Exigir Análisis De Los Resultados

No te conformes con un simple pantallazo o Analytics y 2 frases que no dicen nada. Deberían enviarte un informe más o menos detallado del trabajo realizado en el mes y de los resultados obtenidos. Así como algunas líneas de mejoras y próximos pasos.

Lo bueno del marketing digital es que, como agencia, dispones de gran cantidad de datos que puedes analizar con facilidad; ofreciendo una lectura fácilmente entendible a tus clientes. Si hay cosas que no te quedan claras en el reporte de tu agencia, llámalos para que te lo expliquen de manera que puedas comprender.

4.2.4. Preguntar Por La Publicidad Digital En Google

Hay diversas formas de publicidad online y tu agencia debe de conocerlas y plantearte la opción más adecuada para tu negocio, planteando una estrategia de SEM en base al presupuesto y objetivos acordados.

No confíes en aquellas agencias de publicidad que te ofrezcan resultados rápidos. Y recuerda que lo barato al final termina resultando caro.

Por otra parte, recuerda que todo por lo que estás pagando es tuyo, así que no confíes en aquellas agencias de SEM que se quedan con las propiedades y pide ser tú el propietario de todo, aunque sean ellos quienes lo gestionen.

4.2.5. Pedir Consejo Sobre Redes Sociales

Si te preguntas porqué estás pagando, es fácil. Este es un trabajo, que bien hecho puede impulsar tu negocio, si se suma a una buena estrategia de marketing integral. Y es que aparecer en Facebook, Instagram o Google My Business es gratis, pero no el trabajo de Community Management.

La gestión de redes sociales implica tener un perfil actualizado y comunicarse e interactuar, a través de él, con otros perfiles de interés de una forma adecuada; buscando convertirlos en clientes para tu negocio.

4.2.6. Preguntar Por La Publicidad En Redes Sociales

Lo que no es gratis, es aparecer en forma de anuncio, esto es lo que se denomina un servicio de Social Ads.

Para que esto funcione, y teniendo en cuenta el punto anterior, asegúrate de que han hecho un buen trabajo de segmentación; es decir, que tus anuncios van a verlos personas sobre las que realmente tengas probabilidades de hacer negocio.

4.2.7. Exigir Mejorar Tu Seo – (Search Engine Optimization) Optimización de ingeniería de búsqueda, (SEO) o Posicionamiento En Buscadores

No hay técnicas secretas, ni recetas milagrosas. Que tu página vaya alcanzando cierta relevancia y por ello Google la muestre en mejores posiciones, será consecuencia del tiempo y el esfuerzo.

El posicionamiento funciona a través de las palabras clave o Keywords que tienen relevancia para tu negocio, pero tienes que tener en cuenta que toda tu competencia está luchando por lo mismo.

Lo que de verdad debe hacerte sospechar, es que si el posicionamiento orgánico de tu web o e-commerce no es bueno, el experto en SEO no te pida cambiar en nada de la web. Además lo más lógico es que te pidan acceso al FTP para poder intervenir sin alterar tu web.

4.2.8. Preguntar Por El Gestor Del Servidor Y Dominio Web

Lo primero es saber qué es cada cosa:

Dominio: es el nombre de tu página web, por ejemplo tunegocio.com

Servidor o Hosting: es donde se aloja tu web, con todo su contenido

Tienes que entender que lo que haces con el dominio es alquilarlo, por lo que deberás renovarlo, normalmente cada año; pero que no hay ningún otro tipo de servicio que se le pueda incluir.

Además, una vez tengas tu hosting, podrás crear diferentes cuentas de correo bajo el nombre de tu dominio, por ejemplo oficina@tunegocio.com.

4.2.9. Asegurar, de Que No se Pagara Por Humo,

Este es nuestro último y mejor consejo. Si después de todo esto todavía tienes dudas sobre la agencia de marketing que vas a contratar: infórmate, compara y pregunta. Que no te dejen nada sin resolver.

En Hey Brother somos claros y transparentes, buscando siempre lo mejor para tu negocio. Contáctanos y te haremos una propuesta detallada, específica para tu

negocio; sin florituras. Porque nos gusta hacerte crecer dándote la mejor comunicación.

4.3. ¿Qué son los imperios digitales?

Imperio Digital es una organización política en el que un Estado o Nación impone su poder en otros países por medios digitales, tal como el espionaje, el hackeo a multinacionales, empresas privadas, publicas, corporaciones.

Reclutan a personas jóvenes con la promesa de enseñar los secretos para ganar dinero por medio de una plataforma online de cursos exclusivamente para ayudarte a crecer tu empresa.

La promesa de ganar mucho dinero por internet prometen ganancias de 6 cifras, con la promesa de invertir en un negocio real, aseguran que tienen secretos y estrategias reales, te ofrecen sistemas de ganancia de dinero por internet, venta de x productos mediante agencias de marketing, las empresas te dan un link de afiliado por las ventas que puedes hacer por promover el producto, así podrás ganar una tajada mensual, pero en si son agencias de reclutamiento para especializar a gente en ciberataques

4.4. Que son los negocios Digitales?

Gartner afirma que el negocio digital es la creación de nuevas cadenas de valor y oportunidades de negocio que las empresas tradicionales no pueden ofrecer.

McKinsey enfatiza que "lo digital debe verse menos como algo y más como una forma de hacer las cosas".

Utilizar tecnologías existentes para reducir costes, recopilar datos y proporcionar una mejor experiencia al cliente.

Las empresas digitales se centran en ofrecer ventajas competitivas que la tecnología les da, ya sea reduciendo gastos o proporcionando nuevo valor a sus clientes. Pero esto es otra forma de estafa, porque los que hacen este servicio, no son dueños de la cadena de suministros, por lo tanto no pueden ofrecerte ventajas competitivas en el precio por qué no lo tienen. Simplemente llega a ser una oferta fraudulenta

Adoptar el concepto de transformación digital y los cambios culturales que requiere. La implementación y gestión de servicios digitales puede requerir una reestructuración organizacional, especialmente a medida que se crean nuevos roles y se da mayor atribución a las decisiones estratégicas de IT.

Bajo este criterio ofrecen ellos sus servicios, sus conocimiento su experiencia con la promesa de mayor ganancias, pero lo que realmente están haciendo es explorar nuevas oportunidades de inversión sacando información a los que aceptan ese tipo de servicio, se denomina Espionaje Comercial, en el cual casi nunca se materializa los conocimientos ofertados por dicho experto

Explorar nuevos modelos de negocio que pongan la experiencia del cliente en el centro de la estrategia digital. La gente a menudo está dispuesta a gastar más por una experiencia de cliente excepcional, haciéndolo un diferenciador clave en la economía digital. Los modelos empresariales que se alinean con un enfoque hacia la satisfacción del cliente se centrarán en los servicios digitales, ya que lo digital es la experiencia cada vez más preferida por los usuarios. Todos estos servicios encierran un interés, que al final llega a concretarse en estafa por medios digitales

4.5. Negocio multinivel, esquema multinivel digitales en base a comisiones.-

La posibilidad de ser su propio jefe, generar un buen ingreso, trabajar un horario flexible, liderar un equipo y hasta posiblemente tener su propio sitio de ventas en línea. Si tienes un alma emprendedora parecería ideal, ¿verdad?

De hecho, muchos lo intentan mediante las compañías de mercadeo multinivel

Un modelo de negocio en el que empresas usan a distribuidores independientes para realizar ventas directas al público de sus productos o servicios.

La realidad es que la mayoría fracasan y no generan ganancias. Incluso, pierden dinero.

Quienes lo logran es porque no solo hacen ventas propias, sino que tienen un equipo de vendedores que les genera comisiones —de ahí que se denominen empresas “multinivel”

4.6. Sistema piramidal digital

“En el esquema clásico "piramidal", los participantes intentan ganar dinero solamente mediante el reclutamiento de nuevos participantes, y generalmente:

El promotor promete un alto retorno en un período corto;

No se vende ningún producto o servicio real; y

El énfasis principal se hace sobre el reclutamiento de nuevos participantes”(https://www.investor.gov/esquemas-piramidales)

Con frecuencia, los estafadores promueven los esquemas piramidales a través de las redes sociales, publicidad en Internet, sitios web de empresas, presentaciones grupales, conferencias telefónicas, videos en YouTube y otros medios. Los promotores del esquema piramidal pueden esforzarse mucho para hacer que el programa luzca como un negocio, como un programa de mercadeo de múltiples niveles (MLM, en inglés) legítimo. Pero los estafadores usan el dinero que pagan los nuevos reclutados para pagar a inversores de etapas anteriores (por lo general, también reclutados). En este punto, los esquemas se hacen demasiado grandes, el promotor no puede recaudar suficiente dinero de los inversores nuevos para pagar a los inversores anteriores y las personas pierden dinero.

4.7. Estas son algunas las características del esquema piramidal:

4.7.1. Énfasis en el reclutamiento.

Si un programa se enfoca solamente en reclutar a otros para que se unan al programa sin costo, probablemente se trata de un esquema piramidal. Sea escéptico si recibe más compensación por reclutar a otros que por ventas de productos.

4.7.2. No se realiza venta de ningún producto o servicio real.

Sea precavido si lo que se vende como parte del negocio es difícil de valorar, como los denominados servicios o productos "tecnológicos", como libros electrónicos de licencia masiva o publicidad en línea en sitios web poco usados. Algunos estafadores eligen "productos" que parecen sofisticados para que sea más difícil demostrar que la empresa es un esquema piramidal fraudulento.

4.7.3. Promesas de retorno económico alto en un período cortó.

Sea escéptico de promesas de dinero rápido; podría significar que se pagan comisiones del dinero de los nuevos reclutados y no a partir de las ganancias generadas por ventas de productos.

4.7.4. Dinero fácil o ingreso pasivo (no se requiere la intervención de uno para generar dinero).

No existe un almuerzo gratis. Si se le ofrece compensación a cambio de hacer poca cosa, como hacer pagos, reclutar a otros o poner publicidad en línea en sitios web dudosos, es posible que sea parte de un esquema piramidal ilegal.

4.7.5. No hay ganancias demostradas de ventas al por menor.

Solicite ver documentos, como declaraciones financieras auditadas por un contador público certificado (CPA, en inglés), que demuestren que la empresa genera ganancias de la venta de productos o servicios a personas que no pertenecen al programa. Como regla general, las empresas de MLM legítimas derivan sus ingresos principalmente de la venta de productos, no de reclutar miembros.

4.7.6. Estructura de comisiones de ganancia compleja.

Preocúpese a menos que las comisiones se basen en productos o servicios que usted o sus reclutados venden a personas que no pertenecen al programa. Si no entiende cómo se le compensará, sea precavido.

4.7.7. Todos los esquemas piramidales colapsan, tipo (Pasanako en territorio Boliviano)

Cuando los estafadores intentan hacer dinero solamente reclutando nuevos participantes en el programa, eso es un esquema piramidal y solo hay un resultado matemático posible: el colapso. Imagine si un participante debe encontrar a otros seis participantes, quienes, a su vez, deben reclutar a seis personas cada uno. En solo 11 capas de la línea descendiente de la organización, usted necesitaría más participantes que toda la población de Estados Unidos para

mantener el esquema. Este gráfico informativo muestra cómo todos los esquemas piramidales están destinados al colapso.

4.8. Campañas digitales fraudulentas en redes sociales

Según la BBC Las redes sociales son el lugar ideal para que los delincuentes de internet encuentren víctimas para sus estafas.

Además de tener millones de usuarios, admiten aplicaciones de software abierto.

Así, cualquier programador más o menos experimentado puede escribir un código malicioso que funcione en estas plataformas y con el que pueda engañar a los usuarios.

Los fraudes suelen consistir en ofrecer productos o servicios que el usuario nunca recibe.

Pero en el proceso para conseguir los premios o regalos prometidos, suele abrir las puertas a virus o malware, o entrega sus datos personales.

Los ciberdelincuentes o bien comercializan con ellos o suscriben a las víctimas a servicios de mensajería denominadas premium.

Así, cuando aún sin saberlo están inscritos a estos, reciben mensajes con música, juegos, concursos, noticias, campañas y otro tipo de contenidos a un costo superior al de los SMS convencionales.

Hay fraudes de todo tipo, pero te presentamos los cuatro que más están circulando en los últimos tiempos.

4.9. Cupones de descuento

Si te están ofreciendo cupones de descuento de US$500 a cambio de que contestes a unas cuantas preguntas, sospecha. Es lo que advierte la empresa de seguridad en internet Kapersky Lab.

Quienes llevan a cabo estas estafas suelen utilizar como gancho el nombre de empresas conocidas.

Incluso suelen crear páginas de internet ficticias de las empresas para hacer las campañas más creíbles.

Y la dinámica suele ser siempre la misma: piden que se responda a una encuesta, después solicitan que se comparta, y por último dicen que requieren de tus datos para poder enviar el supuesto cupón.

Éste nunca llega, pero lo que el usuario sí podría recibir es una factura más elevada a finales de mes.

4.10. Solicitudes de "phishing", falsos agentes de cobranza por medio del internet

"Alguien acaba de publicar una foto tuya", dice el mensaje que acabas de recibir.

Como quieres ver la imagen en cuestión, haces clic en el enlace adjunto.

Éste te lleva a la página de inicio de una sesión de Twitter o Facebook, así que introduces tu usuario y tu contraseña.

Y cuando lo haces, un delincuente cibernético obtiene tus datos, porque la página de acceso a las redes sociales era falsa.

4.11. Mensajes de voz de WhatsApp

Es posible que hayas recibido un correo electrónico advirtiendo que uno de tus contactos te dejó un mensaje de voz en WhatsApp e invitándote a descargarlo.

Cuidado, es un fraude, advierten los expertos de Kapersky Lab.

Si caes en la trampa y tratas de reproducirlo o descargarlo, abrirás la puerta a un malware que se instalará en tu equipo.

La propia empresa advierte que se trata de una estafa.

En su página de internet, WhatsApp aclara que no envían mensajes de texto ni correos electrónicos, a no ser que el usuario se haya puesto en contacto anteriormente con el equipo de soporte.

4.12. Notificaciones de envío de paquetería

Es un sistema similar al del fraude de los cupones de descuento.

Recibes un mensaje en nombre de una empresa de paquetería en el que se te notifica un envío.

Si no esperas ningún paquete, lo más probable es que sea un fraude.

En ese caso llevará adjunto un fichero con código malicioso.

Para no sucumbir a esta estafa, los expertos dicen que basta con comprobar el remitente, ya que no suele coincidir con el de la empresa de paquetería.

En cuanto al resto, Kapersky Lab recomienda ser cauteloso y desconfiar siempre de promociones y de concursos.

Así, si te encuentras con la promoción de una marca conocida en las redes sociales, los expertos en seguridad te aconsejan comprobar si existe en el perfil de la empresa en Facebook o Twitter.

También señalan que conviene prestarle atención al URL de la página web a la que remite la promoción, sobre todo si está acortado, y desconfiar de los errores ortográficos.

Por su parte, Norton, la división de antivirus de la empresa de seguridad en internet Symantec, recomienda no incluir información personal como el correo electrónico o el número de teléfono al crear o actualizar el perfil en una red social.

Asimismo, los expertos en seguridad de internet señalan que deberías tener cuidado con los correos que advierten del cierre de cuentas de Facebook o Hotmail; con los que informan de la muerte de algún personaje famoso; con las solicitudes de donaciones; y con cualquier enlace que te pide confirmar tu cuenta agregando tu usuario y contraseña. (https://www.bbc.com/mundo/video_fotos/2015/09/150915_tecnologia_estafas_redes_sociales_lv).

4.13. Comercio electrónico Fraudulento?

El e-commerce, o comercio electrónico, es un sistema de compra y venta de productos o servicios que se realiza exclusivamente a través de Internet. Se refiere a las transacciones entre compradores y vendedores mediante una plataforma online que gestiona los cobros y los pagos de manera completamente electrónica.

Este tipo de actividad, contiene, diversas variantes de fraude electrónico, como oferta de productos que no hay en el mercado o son productos ilícitos, que estas organizaciones, proponen la compra o la venta, de dichos productos, como son productos ilícitos, no existe la trazabilidad de la transacción, es más muchas veces lo que uno adquiere nunca llega a su destino, convirtiéndose en una compra o venta fraudulenta.

4.14. Que es la piratería de software?

Es la apropiación indebida de programas, y patentes y derechos de autor, es un delito transfronterizo de amplia difusión en el mundo entero, La piratería informática es un problema importante para las empresas fabricantes de software que ven cómo cada año una buena parte de sus ingresos se volatilizan por este motivo en especial el software de carácter militar que comprende patentes militares de gran valor económico y estratégico de los países vulnerando la seguridad cibernética.

“Es cuando una obra artística, literaria, científica, fonética, tecnológica o audiovisual, es vulnerada por otras personas al:

Descargar o subir información que tienen derechos autor sin poner las referencias respectivas o sin pagarla.

Utilizar o modificar información para finalidades comerciales o de propaganda.

Usurpar códigos de programación de desarrolladores independientes (apps, programas, plantillas web, entre otros).

Instalar programas informáticos en ordenadores o portátiles sin pagarlos.

Todas estas situaciones y otras, son considerados como actos de piratería en Colombia, por violación a los derechos de autor.” (https://www.agtabogados.com/blog/que-es-la-pirateria-digital-y-derechos-de-autor-en-colombia/).

5. Capitulo IV

5.1. Marco Normativo

Los Marcos Normativos son un conjunto de leyes, normas y reglamentos que son aplicables a las funciones o actividades que se planea llevar a cabo y que deben ser identificados para que las actividades se realicen de manera armónica, sin incurrir en riesgos de tipo legal.

- Ley de Privilegios Industriales del 12 de diciembre de 1916
- Ley reglamentaria de marcas de 15 de enero del 2018
- Constitución Política del Estado Plurinacional de Bolivia de 2009
- Ley nº 1768 de 10 de marzo de 1997 actualizado por ley nº 2492 de 4 de agosto de 2003
- Ley nº 1322 de 13 de abril de 1992 sobre derechos de autor (protección Jurídica de software)
- Ley nº 1430 de 11 de febrero de 1993, aprueba y ratifica la Convención Americana sobre Derechos Humanos, " Pacto de San José de Costa Rica" suscrita en San José Costa Rica, el 22 de noviembre de 1969
- Ley nº 1438 de 12 de febrero de 1993, de adhesión al Convenio que establece la Organización Mundial de la Propiedad Intelectual
- Ley nº 1449 de 15 de febrero de 1993, por el que se regula el ejercicio de la profesión de la ingeniería y actividades afines , en todas sus ramas y actividades, así como la propiedad intelectual sobre los documentos técnicos.
- Ley nº 1428 de 6 de abril de 1993 Convenio de la Unión de Paris (CUP)
- Decisión 244: Regimen Comun sobre Propiedad Industrial de 21 de octubre de 1993. (Common Regime on Industrial Property)
- Decisión 351: régimen Común Andino sobre Derechos de Autor y Derechos Conexos de 17 de diciembre de 1993 (de aplicación preferente con respecto a la norma nacional) (Commmon Provisions on Copyright an neighboring Rights).
- Decisión 391: Régimen Común sobre Acceso a los Recursos Genéticos (Common Regime on Acces to Genetic Reourses).
- Decreto Supremo nº 23907 del 7 de diciembre de 1994 (reglamento ley de derechos de Autor)
- Ley nº 164 de 8 de agosto de 2011.- ley general de Telecomunicaciones, Tecnologías de Información y Comunicación
- Ley nº 1637 de 5 de julio de 1995 Acuerdo sobre aspectos de propiedad Intelectual Relacionado con el Comercio (ADPIC)
- Decreto Supremo nº 1391de 24 de octubre de 2012, Reglamento de ley de telecomunicaciones
- Decreto Supremo nº 24297 de 18 de mayo de 1996 .- Los actuales operadores y proveedores de servicio de telecomunicaciones, cuyas concesiones, licencias, autorizaciones y registros se encuentren vigentes y

hayan sido otorgados conforme a ley, deberán presentar sus solicitudes de adecuación a la Superintendencia de Telecomunicaciones.

- Ley de Modificación del Código Penal nº 1768 de 10 de marzo del 1997
- Decreto Supremo 24581, de 25 de abril de 1997 que crea el Comité Institucional de Protección y Defensa dela Propiedad Intelectual
- Decreto Supremo nº 24582 de 25 de abril de 1997. Reglamento del Soporte Lógico o Software.
- Decreto Supremo nº 24778 de 31 de julio de 1997 Modificase los artículos 7,8,17,22,33,45,46,48,51,53,80,83,86,113,119,120,123,144,145,147,149,150,151,163,164,166,203,205,207,221,223,239,240,241,286,299,305,320, del Reglamento Aprobado mediante Decreto Supremo nº 24132 de 27 de septiembre de 1995 (ley 1632 Telecomunicaciones) (abrogado por Decreto Supremo nº 1391 de 24 de octubre de 2012)
- Decreto Supremo nº 25308 de 23 de febrero de 1999. Se modifica el artículo 173 del Decreto Supremo nº 24132 de 27 de septiembre de 1995 (reglamento a la ley 1632 Telecomunicaciones)
- Proyecto de Ley de Comercio Electrónico, de 31 de diciembre 2001
- Decreto Supremo nº 26553 de 19 de marzo del 2002 marco legal e institucional para la implementación de Nuevas tecnologías de información y Comunicación
- Decreto Supremo nº 26624 del Consejo de ministros, Reglamentación para el registro de dominios ccTCD.BO, de 14 de mayo de 2002 (abrogado por Decreto Supremo nº 1391 de 24 de octubre del 2012
- Proyecto de Ley de transparencia y Acceso a la información Pública de agosto de 2008
- Decreto Supremo nº 214 de 15 de julio 2009 De Política Nacional de Transparencia y lucha contra la corrupción
- Decreto Supremo nº 353 de 4 de noviembre de 2009, Decreto de registro obligatorio y gratuito de los celulares.
- Ley nº 164 de 8 de agosto de 2011 Ley General de Telecomunicaciones, tecnologías de información y Comunicación.
- Decreto supremo nº 1793 de 13 de noviembre de 2013 Reglamento de la ley nº 164.

6. Capítulo V

6.1. Análisis De Los Hechos.-

6.1.1. Pasos para efectuar un análisis de la norma que pretende regular este tipo de actividad delictiva

Se busca la razonabilidad de la norma, también se busca la interpretación de la norma y luego la aplicación de la norma a cada caso,

6.2. Introducción.-

El presente análisis de El Delito de Estafa Digital, utiliza, como paso de análisis el **supuesto del hecho** (Hipótesis anticipada de posible realidad a regular), y como acto resultante la **Consecuencia Jurídica**, que se materializada en la sanción que se pretende efectuar en un proyecto normativo, a partir de las siguientes conceptualizaciones.

6.3. ¿Qué es un BIN Número de Identificación Bancaria de la Posible Victima?

Significa Bank Identification Number por sus siglas en inglés. Un bin son los primeros 6 dígitos (o más) de una tarjeta de crédito/debito (credit card = cc) real, es decir, con un dueño físico.

Por obvias razones, las tarjetas generadas a partir de un bin, NO SON DE PERSONAS REALES, solo son algoritmos ya que, de otra manera, estaríamos usando tarjetas reales todo el tiempo y habría robos sobre las tarjetas de los usuarios todos los días, de esta manera mucha gente estaría en la cárcel por el simple hecho de “binear”.Así que, desde este momento, la estafa digital no es para el usuario dueño de la tarjeta de donde sacaste el bin sino para la empresa donde lo usas, por lo cual se comete un fraude al evadir la seguridad con el método de pago, pero no un robo.

6.4. ¿Qué es una conexión VPN (Red privada virtual), para qué sirve y qué ventajas tiene?

Esta Red Privada Virtual tiene la facilidad de invisibilizar la computadora desde donde se emite el ataque cibernetico el TCP/IP (protocolo de transmisión de control de internet) es una dirección única que identifica a un dispositivo en Internet, al ser invisibilizado, no tiene ubicación exacta en cualquier territorio. Y da la apariencia de ser un ataque cibernético transfronterizo.

Muy aplicado por los Hackers (manipuladores informáticos) para cometer delitos informáticos de diversa variedad. Originalmente creado por el departamento de Defensa de EEUU con fines de aplicabilidad en el espionaje industrial y militar.

Vamos a explicar qué es una conexión VPN, para qué sirve y qué ventajas tienen. Las conexiones VPN no son ni mucho menos un invento nuevo, pero es ahora cuando están empezando a coger tracción entre el gran público.

Precisamente esa versatilidad de la que hablábamos es la misma que crea alguna que otra confusión sobre qué son exactamente estas VPN, pues cada vez más se relaciona a las conexiones VPN con "el mal" (con grandes comillas), pues algunas de sus aplicaciones incluyen el salto de los bloqueos geográficos, un mayor anonimato en la Red o incluso el bloqueo de la publicidad.

VPN son las siglas de Virtual Private Network, o red privada virtual que, a diferencia de otras palabras informáticas más crípticas como DNS o HTTP, sí nos dan pistas bastante precisas sobre en qué consisten.

La palabra clave aquí es virtual, pues es esta propiedad la que genera la necesidad de la VPN en sí, así como la que permite a las conexiones VPN ofrecerte los múltiples usos que veremos más adelante.

Esto es una red local, un conjunto de dispositivos conectados de tal modo que puedan compartir archivos e impresoras sin necesidad de pasar por Internet.

Una conexión VPN lo que te permite es crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet. Es el componente "virtual" del que hablábamos antes. Obtienes las ventajas de la red local (y alguna extra), con una mayor flexibilidad, pues la conexión es a través de Internet y puede por ejemplo ser de una punta del mundo a la otra.

Sin embargo, es otra peculiaridad de las conexiones VPN la que las está volviendo tan de moda hoy en día: los túneles de datos. Normalmente, mientras usas Internet tu dispositivo se pone en contacto con tu proveedor de Internet, que es el que conecta con los distintos servicios web para ofrecerte, por ejemplo, los vídeos de YouTube.

Cuando te conectas a una conexión VPN, esto cambia. Todo tu tráfico de red sigue yendo desde tu dispositivo a tu proveedor de Internet, pero de ahí se dirige directo al servidor VPN, desde donde partirá al destino. Idealmente la conexión está cifrada, de modo que tu proveedor de Internet realmente no sabe a qué estás accediendo. A efectos prácticos, tu dirección IP es la del servidor VPN: en muchos aspectos es como si estuvieras físicamente ahí, conectándote a Internet.

Con el apogeo de Internet y la picaresca tanto de los proveedores de contenidos como de los usuarios, se han ido popularizando otros usos más lúdicos de las conexiones VPN, muchos de ellos relacionados con un concepto muy sencillo: falsear dónde estás.

Al conectarte con VPN, tu dispositivo se comunica con el servidor VPN, y es éste el que habla con Internet. Si tú estás en China y el servidor VPN está en Estados Unidos, generalmente los servidores web creerán que estás navegando desde este país, dejándote acceder a los contenidos disponibles solo allí, como podría ser Netflix.

De igual modo, esta misma lógica se puede usar para acceder a aquellos contenidos que estuvieran censurados o bloqueados en tu país, pero no allí donde se encuentra el servidor VPN. Así es como millones de ciudadanos chinos logran conectarse a Facebook y otras 3.000 webs bloqueadas en el país.

Capa extra de seguridad

Aunque no es estrictamente necesario, sí es común que las conexiones VPN vengan acompañadas de un cifrado de los paquetes que se transmiten con ellas, por lo que es normal la recomendación de que, si necesitas conectarte a un punto de acceso Wi-Fi público, al menos uses te conectes con una VPN.

Ahora que ya sabemos qué es una conexión VPN y para qué sirve, es hora de resumir una lista de las ventajas e inconvenientes que te supone el uso de esta tecnología. Primero, la parte positiva:

Funciona en todas las aplicaciones, pues enruta todo el tráfico de Internet, a diferencia de los servidores proxy, que solo puedes usar en el navegador web y un puñado de aplicaciones más que te dejan configurar las opciones de conexión avanzadas.

Se conecta y desconecta fácilmente. Una vez configurado, puedes activar y desactivar la conexión a tu antojo.

Seguridad adicional en puntos de acceso Wi-Fi, siempre y cuando la conexión esté cifrada, claro

Falseo de tu ubicación, como ya hemos visto en el apartado anterior, una conexión VPN es un modo eficaz de evitar la censura o acceder a contenido limitado a cierta región.

Tu proveedor de Internet no puede saber a qué te dedicas en Internet. ¿No te apetece que tu proveedor de Internet sepa que te pasas horas viendo vídeos de gatitos en YouTube? Con una VPN no sabrán a que te dedicas, pero ojo, que sí lo sabrá la compañía que gestiona el VPN.

6.5. Que es la Deepweb

La ‘deep web’ o web profunda es un espacio de internet donde está albergado el contenido que no aparece en los motores de búsqueda convencionales, debido a diversos factores que no tienen por qué responder a la ilegalidad. (fuente: Ana Gómez Blanco)

6.6. Que es la Darknet

Que constituye una pequeña parte de la 'deep web', cuyos contenidos sí suelen ser ilícitos. (Fuente: Ana Gomez Blanco)

Es un instrumento de navegación Digital en donde predomina el anonimato, con un acceso libre a cualquier tipo de información y conocimiento informático de los métodos de ataques cibernéticos en los diferentes países y sus estructuras por medio del uso de VPN.

Red oscura, forma parte de la Deep web, son páginas web y servicios a los que no se puede acceder a través de los motores de búsqueda tradicionales (Google, Bing, DuckDuckGo). La darknet está formada por un conjunto de sitio oculto a los que se accede a través de navegadores específicos, como puede ser Tor. De esta forma, los usuarios no solo pueden llegar a las web de la red oscura sino que también pueden mantener una navegación anónima y privada, pues dichos navegadores utilizan diferentes servidores proxy para que su IP sea difícil de rastrear.

6.7. Que es Namso –Gen

Es una base de datos multipropósito, que se ocupa de generar datos para las tarjetas de crédito, haciéndolas vuilnerables para los Ciberataques

6.8. ¿Qué es el Carding?-

Base fundamental para los ciberataques a partir de las tarjetas de crédito o ahorro de los bancos en el mundo.

Uso secuencial de tarjetas de crédito de modo que discrimina las que no están habilitadas, por medio de una exploración digital, y detectan las que si funcionan.

Se trata de una forma de estafa online que consiste en acceder ilegalmente a los datos de una tarjeta, ya sea de débito o de crédito.

Los Bineros es el nombre con el que se autodenominan estas comunidades delictivas. Un tema importante a destacar es el hecho de que están organizados en grupos de redes sociales, donde comparten tips para conseguir los datos de las tarjetas bancarias e incluso venden y compran datos por paquete.

6.9. Algunas características propias de estas comunidades son las siguientes:

Manejan su propio lenguaje, por ejemplo:

Quemar: Tarjeta registrada por el banco que ha sido vulnerada, y que no se puede utilizar para la compra de cualquier ilícito que significa utilizar todos los fondos monetarios de la tarjeta de crédito o débito de la víctima.

Bins: Término derivado de código binario, son los dígitos de las tarjetas bancarias.

Bineros: Es aquella persona que se dedica a este tipo de estafa.

Las compras que realizan no suelen ser muy grandes, por lo regular utilizan los datos para pagar cuentas de Spotify, Netflix, YouTube, Uber, suscripciones mensuales a videojuegos, pasajes de autobús etc.

Están organizados en grupos de Facebook, en donde realizan la compra-venta de bins.

QUE ES UN BIN.- Son los primeros seis números de una tarjeta lo cual identifica al banco y al tipo de tarjeta que es, los Bins permite generar tarjetas de crédito o débito.

Se puede usarla para cualquier tipo de compra que permita una verificación de tarjeta para pago Ej.

- Netflix en la mayoría de los casos se usa el método de pago por paypal.
- Spotify este es sencillo en la mayoría de casos se solicita un vpn para cambiar la ip
- Play Store y App store

- Crunchiroll, páginas pornográficas, Blim, Deezer, Napster, tidal, publicidad en facebook.
- Amazon y Aliexpress entre otros
- Los Bins se usan desde compras virtuales hasta compras físicas.

6.10. Pasos que efectúan los hackers para un un ciberataque (carding)

Este instrumento de manejo ilícito de las tarjetas de crédito, requiere de un previo conocimiento de ingreso a la DepWeb, seguidamente ingreso a la Darknet definidos anteriormente y utilizados secuencialmente estos instrumentos sin ingresar a navegadores que rastrean el IP (protocolo de internet) y la navegación como es el Google, buscando otra opción como es el TOR.(transmisión Onion Red) Red de transmisión tipo cebolla, por capas que dificultan el rastreo del TCP/IP.

Pasos que se efectúan en un ciber ataque de Carding:

- Ingresar a la deepweb, entras a TOR
- Buscar páginas de información específica de acuerdo al ilícito, en este caso páginas dedicadas al Carding
- Habilitar la Red Vpn para obtener anonimato
- Entrar a Namso-Gen.com con el fin de obtener datos de información confidencial de los usuarios de tarjetas de crédito
- una vez generada el BIN bank identification number, se procede a la compra secreta de cualquier ilícito en todo el planeta.
- Él envió de la paquetería producto de la transacción no llega al domicilio del usuario, sino a un lugar público como ser, casilleros de Correos de Bolivia, etc.
- Eliminar el registro de compra de la tarjeta vulnerada o quemada, de modo que no sea rastreada, compartiendo o distribuyendo la información obtenida de la tarjeta a muchos usuarios que son menores de edad que son inimputables ante la ley
- Los menores de edad involucrados en este tipo de actividad, compran productos ilícitos de bajo coste, para que satisfacer sus curiosidades, por ejemplo, ingresan a páginas pornográficas de pago, como ser onlyfans.com, muy peligroso para los usuarios victimas que perdieron su tarjeta de crédito o ahorro, especialmente si son funcionarios públicos, caso Presidente De Colombia, con una amenaza potencial de hackeo por medio del carding a todo el Poder Ejecutivo, motivo por el que se archivó la ley de subida de impuestos en Colombia.

Muchos Funcionarios públicos, no denuncian este ilícito, por temor a la opinión pública, por lo que las victimas de carding entran a ser parte de las cifras negras de dinero estafado digitalmente. Fuente: (Anónima, Difundido por Bots)

6.11. Conclusión del análisis de caso

Después de hacer un amplio análisis investigativo, en el campo del Derecho Informático, mas puntualmente en la **Estafa Digital** con sus diferentes variantes, que son un sin número de **modus operandi** que están en continua evolución, van apareciendo muchas otras formas de Estafa Digital, su dinamismo de este tipo de delito que va cambiando cada instante, hace que la norma tenga que adecuarse a esta forma de Evolución delictiva, que es aplicable por medio de **la Inteligencia artificial,** con el fin de controlar a los sujetos activos del Delito y entren en el anonimato, y no sea posible ser imputables ante la ley. Y para este efecto, el código penal Boliviano debe especializarse, **en Inteligencia Artificial Penal**. A la par crear una **Infraestructura Informática en el estado Plurinacional de Bolivia,** para regular y prevenir este tipo de delitos de ciberataques masivos.

7. Capítulo VI

7.1. Propuesta De La Investigación

7.1.1. Se propone la creación de Infraestructura Informática Para El Estado Plurinacional De Bolivia

7.1.2. ¿Qué es una infraestructura informática?

Es un conjunto de equipos y programas (hardware y software, sobre el que se soportan, los servicios del Estado, como ser la Agencia Estatal Plurinacional de Infraestructura Informática, para cubrir las necesidades de supervisión, control, y optimizar la cooperación interinstitucional y administrativa del Estado.

Se puede definir, como el conjunto de elementos para el almacenamiento de datos del Estado Plurinacional de Bolivia, para optimizar la gestión interna y la seguridad de la información que es la base de la gestión administrativa del Estado.

Componentes de la Infraestructura de tecnología informática plasmados en intranet Estatal, Estos componentes son equipos y programas, (hardware y software):

- Instalaciones
- Centros de datos de nivel central, departamental , municipal y regional
- Servidores,
- Computadoras de escritorio,
- Hardware de redes, intranet estatal conectado a todos los niveles de gobierno
- Software de aplicaciones dedicados al gobierno electrónico plurinacional

Infraestructura Hiperconvergente (HCI).- es un sistema unificado aplicable en el Estado Plurinacional de Bolivia y definido por software que reúnen todos los elementos de un centro de datos tradicional:

- Almacenamiento
- Recursos informáticos

- Redes
- Gestión de datos

7.1.3. ¿Cuáles son los elementos de la infraestructura informática?.-

Incluye todo el acervo físico y material que sustenta y facilita el desarrollo productivo de un país, se incluye elementos como:

- Sistemas jurídicos digitales
- Sistemas económicos digitales
- Sistemas de salud digital
- Sistema de educación digital
- Sistema de seguridad interna digital
- Sistema de desarrollo informático para las diferentes instituciones del Estado Plurinacional de Bolivia
- Sistemas de investigación científica digitales
- Sistemas empresariales digitales
- Sistemas meteorológicos digitales
- Sistemas de productividad
- Sistemas de eficiencia
- Abastecimiento de agua y recursos
- Tratamiento de residuos sólidos y aguas servidas
- Telecomunicaciones
- Generación y transmisión de energía
- Sistemas de infraestructura web
- Sistemas de carreteras, vías aeropuertos y vías aéreas
- Sistemas de riego
- Sistemas eléctricos
- Sistemas industriales y tecnologías aplicadas
- Sistemas de ferrocarriles
- Sistemas navieros

7.1.4. ¿Cómo funciona la Hiperconvergencia?

Los sistemas hiperconvergentes, aprovechan la inteligencia artificial, definida por el software, para administrar los sitios de almacenamiento y aprovechamiento y permiten que se ejecute y se gestionen en la misma plataforma de servidor, lo que elimina las ineficiencias de la gestión gubernativa y acelera el procesamiento de la información.

La infraestructura Hiperconvergente HCI utiliza equipos de computación (hardware) como equipos integrados con discos duros o SSD integraos, centralizando la gestión de todas las tareas.

- Virtualización
- Redes
- Almacenamiento de datos

Propios de los centros de datos, la Híper convergencia, combina recursos informáticos, almacenamiento de datos y redes de todos los sistemas, en un solo sistema híper convergente

7.1.5. ¿Qué es la infraestructura web?

Es la integración de almacenamientos con la potencia informática, elimina la complejidad de las pérdidas de rendimiento en las redes de almacenamiento y permite ampliar la infraestructura de servidor en servidor

7.1.6. ¿Qué es el Big Data?

Big Data es un término que describe el gran volumen de datos, tanto estructurados como no estructurados, que cubre la administración del Estado diariamente, pero no es la cantidad de datos lo que es importante. Lo que importa con el Big Data es lo que las instituciones administrativas hacen con los datos. Big Data se puede analizar para obtener ideas que conduzcan a mejores decisiones y movimientos, estratégicos.

Cuando hablamos de Big Data nos referimos a conjuntos de datos o combinaciones de conjuntos de datos cuyo tamaño (volumen), complejidad (variabilidad) y velocidad de crecimiento (velocidad) dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales, tales como bases de datos relacionales y estadísticas convencionales o paquetes de visualización, dentro del tiempo necesario para que sean útiles. Fuente: (https://www.powerdata.es/big-data)

La naturaleza compleja del Big Data se debe principalmente a la naturaleza no estructurada de gran parte de los datos generados por las tecnologías modernas, como los web logs, la identificación por radiofrecuencia (RFID), los sensores incorporados en dispositivos, la maquinaria, los vehículos, las búsquedas en Internet, las redes sociales como Facebook, computadoras portátiles, teléfonos inteligentes y otros teléfonos móviles, dispositivos GPS y registros de centros de llamadas.

En la mayoría de los casos, con el fin de utilizar eficazmente el Big Data, debe combinarse con datos estructurados (normalmente de una base de datos relacional) de una aplicación comercial más convencional, como un ERP (Enterprise Resource Planning) o un CRM (Customer Relationship Management).

7.1.7. Importancia del Big Data

Lo que hace que Big Data sea tan útil para muchos Estados es el hecho de que proporciona respuestas a muchas preguntas que las instituciones administrativas ni siquiera sabían que tenían. En otras palabras, proporciona un punto de referencia. Con una cantidad tan grande de información, los datos pueden ser moldeados o probados de cualquier manera que El Estado considere adecuado.

Al hacerlo, las instituciones administrativas del Estado son capaces de identificar los problemas de una forma más comprensible.

La recopilación de grandes cantidades de datos y la búsqueda de tendencias dentro de los datos permiten que las Instituciones Administrativas del Estado se muevan mucho más rápidamente, sin problemas y de manera eficiente. También les **permite eliminar las áreas problemáticas como por ejemplo el proyecto de ley de Legitimación de Ganancias Ilícitas** antes de que los problemas acaben con sus beneficios o su reputación.

El análisis de Big Data ayuda a las instituciones administrativas del Estado a aprovechar sus datos y utilizarlos para identificar nuevas oportunidades.

Eso, a su vez, conduce a movimientos de regulación normativa más inteligentes, operaciones más eficientes, mayores ganancias y ciudadanos más felices. Las instituciones administrativas del Estado Plurinacional con más éxito con Big Data consiguen valor de las siguientes formas:

7.1.7.1. Reducción de coste.

Las grandes tecnologías de datos, como Hadoop (base de datos de software libre) y el análisis basado en la nube, aportan importantes ventajas en términos de costes cuando se trata de almacenar grandes cantidades de datos, además de identificar maneras más eficientes de hacer negocios.

7.1.7.2. Más rápido

Mejor toma de decisiones. Con la velocidad de Hadoop y la analítica en memoria, combinada con la capacidad de analizar nuevas fuentes de datos, las empresas pueden analizar la información inmediatamente y tomar decisiones basadas en lo que han aprendido.

7.1.7.3. Nuevos productos y servicios.

Con la capacidad de medir las necesidades de los clientes y la satisfacción a través de análisis viene el poder de dar a los clientes lo que quieren. Con la analítica de Big Data, más empresas están creando nuevos productos para satisfacer las necesidades de los clientes.

7.1.7.4. ¿De qué manera?

Identificando y señalando, que normativa es la más adecuada para este tipo de delitos, a nivel internacional para lo cual proponemos la creación de las siguientes instituciones jurídicas y administrativas:

7.1.7.5. Se propone la creación de una secretaria de comercio Digital interior de Bolivia (proyecto de ley).-

Al ser un defensor de los intereses de las empresas Del Estado Plurinacional de Bolivia. Éste creará los estándares industriales y registrará marcas y patentes.

La misión del Departamento es crear las condiciones para el crecimiento económico y las oportunidades.

El Departamento de Comercio promoverá la creación de empleo y el crecimiento económico asegurando el comercio justo, proporcionando los datos necesarios

para apoyar el comercio y la democracia constitucional, y fomentando la innovación al establecer estándares y realizar investigación digital y desarrollo fundamentales. (Fuente: https://www.commerce.gov/about)

Ayudará a negociar acuerdos comerciales bilaterales y hace cumplir las leyes que garantizan la igualdad de condiciones para las empresas y los trabajadores Bolivianos.

7.2. Políticas aplicables para la creación de la Secretaria De Comercio Interior Del Estado Plurinacional de Bolivia mediante ley.

7.2.1. Políticas de redes sociales y web 2.0

El Departamento de Comercio Interno a crearse en el Estado plurinacional de Bolivia mediante una ley, estará comprometido a operar todas sus comunicaciones y transacciones con individuos y organizaciones de una manera abierta y transparente. Los servicios de redes sociales y Web 2.0 (SM / W2.0) son una vía cada vez más importante para que las partes interesadas y los miembros del público interactúen con este Departamento de Comercio Interno Plurinacional de Bolivia de manera eficiente, eficaz y transparente.

7.2.2. Estrategia digital.-

Para que los conjuntos de datos de Comercio Interior ahora estárán integrados en un archivo Plurinacional.

7.2.3. Calidad de la información.-

Para la aplicación de esta política gubernamental protéctiva, se sugiere implementar un proyecto de ley que instrumente la calidad, objetividad, utilidad e integridad de la información en base a la creación de Una Institución De La Información Científica, Técnica, Estadística del Estado Plurinacional de Bolivia.

Los programas Hidrológicos y atmosféricos de Comercio Interno mejoran la comprensión y el uso racional del medio ambiente natural para promover la seguridad, el bienestar y el comercio de la nación.

Estas responsabilidades incluirán predecir el clima, trazar los ríos y lagos proteger los humedales y las áreas ecológicas y geográficas.

A nivel nacional, los programas de Comercio Interno promoverán empresas comerciales a largo plazo que crearán puestos de trabajo para grupos minoritarios y en áreas subdesarrolladas del Estado Plurinacional de Bolivia. Estos programas estarán respaldados por informes, publicaciones, proyecciones y experiencia empresarial. El Departamento de Comercio Interno brindara servicios a ciudadanos y empresas privadas, así como a gobiernos estatales, locales y tribales.

7.2.4. Código fuente abierto.-

Código Fuente Plurinacional De Bolivia, Esta política entrara en vigencia de inmediato, si se aplicará a todos los proyectos que se encarguen del desarrollo de software personalizado dentro del Departamento de Comercio interno del Estado Plurinacional de Bolivia para incluir todas las Unidades Operativas y Administrativas.

7.2.5. Lenguaje simple

Se propone la creación de Proyecto de Ley de Redacción del Estado Plurinacional de Bolivia, para que en los contratos no exista letra pequeña o clausulas digitales fraudulentas o susceptibles de engaño o estafa.

7.2.6. Archivo de políticas de TI (tecnología de la Información)

Estos conceptos podrían ser fundamentos para poder redactar nuevas normas dentro del código penal, nuestro código penal es acusatorio, y sancionador por que se basa en la tipificación, antijuricidad, culpabilidad y punibilidad elementos del delito que en la actualidad no son suficientes, básicamente debería ser la norma primero previsionista, con políticas proteccionistas para las personas naturales y jurídicas, en el ciudadano no sea vulnerable, ante las estafas digitales.

7.2.7. Creación de la Comisión Plurinacional de Comercio Digital Boliviano.- (como proyecto de ley)

Sera responsable de asegurar que el mercado interno de consumo sea eficiente y no tenga restricciones. La Comisión hará cumplir las leyes Plurinacionales de protección a los consumidores y las leyes de antimonopolio y competencia.

7.2.8. Tipificación para el código penal sobre Estafa o Fraude Digital de valores. (Propuesta de enmienda en el código penal boliviano)

“Es cuando el inversionista ha sido una víctima de engaños monetarios, malas interpretaciones de valores, exceso de compras y ventas, recomendaciones incorrectas, y otros actos que por razones de incompetencia, negligencia o ambición por parte del corredor de bolsa y Firmas de Inversión”. Fuente: (https://investorlawyers.com)

7.2.9. Tipificación para el código penal sobre Asesor de inversiones digitales fraudulentas. (Propuesta de enmienda en el código penal boliviano).

“Las personas mayores suelen ser objeto de fraudes de inversiones porque en muchos casos cuentan con ahorros y bienes. Los fraudes de inversiones pueden ser desbastadores para la estabilidad financiera que tanto trabajo les costó adquirir.

Los fraudes de inversiones consisten en las prácticas engañosas usadas para convencer a la persona de que invierta dinero. Los fraudes pueden ser con valores de la bolsa, bonos, notas, productos básicos, monedas o incluso hasta bienes raíces. El embaucador puede dar información incierta o errada acerca de inversiones reales o inventar una oportunidad falsa.

El embaucador en inversiones puede ser desde un operador de ventas telefónicas hasta un asesor financiero. Es inteligente, sociable, encantador y persuasivo. Hace todo lo posible por ganar su confianza para que usted no investigue antes de invertir.”

(Fuente: https://www.tn.gov/attorneygeneral/working-for-tennessee/consumer/resources/materials/investment-scams-sp.html).

También puede ser solamente un Bot, (Computadora Robot) o un chatBot el que utiliza estos métodos, para que el embaucador obtenga anonimato

7.2.10. Tipificación para el código penal sobre Fraude postal digital. (Propuesta de enmienda en el código penal boliviano)

“Es una confabulación destinada a obtener dinero, o algo de valor, mediante la oferta de algún producto, servicio u oportunidad de inversión que promete más de lo que cumple. Los fiscales deben comprobar que se efectuaron declaraciones falsas en forma intencional y que se utilizó el correo para llevar a cabo ese acto de conspiración.

A pesar de que la mayoría de las empresas de pedidos por correo son honestas y respaldan sus productos y servicios, hay, desafortunadamente, algunas manzanas podridas que echan a perder la reputación de quienes hacen publicidad por correo directo. Estas personas engañan a la gente con ofertas de productos que no tienen ninguna utilidad o valor, curanderismo médico e ideas para enriquecerse de golpe. Algunos son piratas que reciben el dinero y no envían nada de lo prometido.

Son tan inescrupulosos que nos les importa aprovecharse de algún cliente confiado. Su lema es “Deja que el cliente se cuide” y usted podría ser ese cliente.

Los autores de fraude postal a menudo se basan en los mismos trucos conocidos. Es probable que usted también esté familiarizado con algunos de ellos. En las siguientes páginas figuran algunas de las estafas y formas más comunes de fraude postal y otros problemas que comúnmente tienen los consumidores. Estén atentos para reconocerlos.

Sorteos y premios “gratis”

Sucede todos los días. Miles de personas reciben alguna notificación por correo que les informa que han ganado un premio gratis. Usualmente se trata de una tarjeta postal que dice que el premio va a ser uno de cuatro o cinco artículos “valiosos”, como por ejemplo un automóvil, un televisor a color o un bono de ahorro de $1,000.

Típicamente estos avisos provienen de estafadores cuyo único objeto es timar a sus destinatarios. Al comunicarse telefónicamente con la compañía para reclamar el premio, el estafador le responderá que tiene que pagar una quota de “procesamiento o seguro” y le insistirá que le dé un número de tarjeta de crédito. No lo haga. El estafador va a cargar miles de dólares a su cuenta sin autorización alguna. Si se niega a darle un número de tarjeta de crédito, tenga cuidado con la

otra treta que usará para convencerlo de pagar la quota de procesamiento o seguro enviando un cheque por cientos dólares por un servicio de correo privado enviado por la noche o transfiriendo la tarifa a una persona o negocio en Canadá, Costa Rica, u otro país extranjera.

De una u otra manera, tenga la seguridad de que el premio le va a costar más de lo que vale, no va a tener valor alguno o no le llegará nunca.

Consejo de negocios: Muchas compañías han recurrido a la publicidad mediante productos especiales como plumas, llaveros, gorras de béisbol y rasquetas para el hielo, entre otros, para ser más reconocidas. Sin embargo, algunas operaciones ilegales y deshonestas también utilizan estos productos para atrapar a los propietarios y empleados de pequeñas compañías en una confabulación fraudulenta. La estafa empieza con una notificación de que ha ganado un gran premio en un sorteo promocional. Pero hay algo más: le dicen que tiene que comprar una cierta cantidad de artículos con el nombre y logotipo de su compañía para evitar pagar un “impuesto a las donaciones”. La compra, que puede ascender a varios miles de dólares, podría resultar en mercancías de inferior calidad o en nada.”

(Fuente: https://about.usps.com/publications/pub300as/online300as_002.htm)

7.2.11. Tipificación para el código penal sobre Fraude electrónico. (Propuesta de enmienda en el código penal boliviano)

Como el uso de una computadora con el objetivo de distorsionar datos para inducir a otra persona a que haga o deje de hacer algo, que ocasiona una pérdida. Los delincuentes pueden distorsionar los datos de diferentes maneras. Primero, pueden alterar sin autorización los datos ingresados en la computadora. Los empleados pueden usar fácilmente este método para alterar esta información y malversar fondos. En segundo lugar, los delincuentes pueden alterar o borrar información almacenada. Tercero, los delincuentes sofisticados pueden reescribir los códigos de software y cargarlos en la computadora central de un banco para que éste les suministre las identidades de los usuarios. Los estafadores luego pueden usar esta información para realizar compras no autorizadas con tarjetas de crédito.

Fuente:(https://www.law.cornell.edu/wex/es/fraude_cibern%C3%A9tico_e_inform%C3%A1tico).

7.2.12. Tipificación para el código penal sobre Lavado de dinero por medios digitales. (Propuesta de enmienda en el código penal boliviano)

7.2.12.1. Los activos digitales

Una década atrás se creó el bitcoin, la primera criptomoneda concebida, según el papel de su presentación publicado bajo el seudónimo Satoshi Nakamoto, como una cadena de firmas digitales para realizar transacciones electrónicas.

Inicialmente el bitcoin nace como una forma de dinero en efectivo electrónico que permitiría enviar pagos online de manera directa entre las partes, **sin la intermediación de una institución financiera.**

Constituía un proyecto político que abreva en las raíces del cypherpunk, movimiento que combina una aversión anárquica hacia los gobiernos y las grandes empresas con la creencia de que la criptografía puede proteger a las personas contra el control que los gobiernos y empresas realizan de sus datos. Fuente: (Riding the rollercoaster - How to put bitcoin into perspective. The Economist, Aug. 30th 2018.)

En consecuencia, se diseñó un sistema que permitió eliminar la intermediación. La función de registro y depósito, así como la certeza de los saldos en las cuentas, que eviten el doble gasto que, en el caso de la moneda, cumplen las entidades financieras, en el caso del bitcoin, lo suple una red de pares (peer to peer).

Es decir, una red en la cual no hay servidores ni clientes, cada CPU, cumple la función de un servidor conectado entre sí por medio de esta red en el que cada nodo (CPU), administra y optimiza el uso del ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, y obtienen así más rendimiento en las conexiones y transferencias.

Su uso inicial estuvo centrado en la transferencia de archivos y se difundió con las prohibiciones y causas penales iniciadas por violación a los derechos de autor, en el uso de archivos de música.

En el caso de las monedas digitales, esta red de nodos informáticos realiza un registro público de las transacciones, las cuales son validadas, una vez que los nodos se comunican entre sí mediante la red peer to peer (P2P)

Fuente: (https://bitco in.org/fil es/bitcoi n-paper/bitc oin_es.pdf en la referencia N° 1 de este artículo, referida a la red peer to peer, se cita https://es.wikiped ia.or g/wiki/ Peer-to-peer en la que se la define como una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.)

Y llegan a un consenso sobre los estados actuales de la cadena de bloques (blockchain), que cumple la función de registro de un libro mayor.

Fuente: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf.

De esta manera, la creación del bitcoin y de muchos de los demás criptoactivos (en la actualidad hay más de 3000 criptomonedas), estaba dirigido a ampliar el mercado de pagos, con una opción diversa a las monedas fiduciarias, monedas de curso legal de los Estados, sin la intermediación de las entidades financieras.

Por otra parte, su utilización como un instrumento de inversión o de reserva de valor, también prescinde de los agentes de registro y custodia de estos títulos (Caja de Valores, Euroclear, DCV, etc.).

Sin embargo, la volatilidad de su valor, hasta el momento, impactó en un bajo uso para su propósito original, a la vez que alimentó el apetito de los especuladores.

En cualquier medida, la irrupción de las criptomonedas, como un nuevo instrumento de intercambio, generó alteraciones en el mapa de riesgos de los sujetos que, en los términos de la, están obligados, en su ámbito de actuación, a inscribirse ante la UIF Res. UIF N° 50/11 (B.O. 1-4-11).

Y a reportar a la Unidad de Información Financiera (UIF), las conductas o actividades de las personas humanas o jurídicas que pudieran considerarse susceptibles de configurar un hecho u operación sospechosa de lavado de activos o financiación de terrorismo.

La nómina de los sujetos obligados está consignada en el artículo 20 de la citada ley, con sus 23 incisos que incluyen, entre otros, a las instituciones financieras y actividades y profesiones no financieras allí designadas.

Por supuesto que, el uso que en cada momento se dé a estos valores, incidirá de forma relevante en la elaboración de las evaluaciones y de los mapas de riesgos, así como en la regulación de los sujetos obligados; de igual modo, las características y finalidad que se le atribuya a la regulación, condicionará e incidirá en el desaliento o incentivo de su utilización.

Las criptomonedas no sólo generaron cambios en las operaciones de los sujetos obligados, al introducirse la posibilidad de utilización de un nuevo medio de intercambio en sus transacciones, sino que también, en sí mismas, significaron la aparición de un nuevo sector, con nuevos actores, o empresas involucrados en el negocio. Este es el caso de los usuarios, exchanger, administradores y mineros.

Cada uno de estos participantes fueron definidos en un dictamen de la Red de Control de Delitos Financieros del Departamento del Tesoro de Estados Unidos de los Estados Unidos (Financial Crimes Enforcement Network -FINCEN), organismo dedicado a la inteligencia financiera, con la finalidad de evitar la utilización ilícita del sistema financiero y combatir el lavado de dinero.

En el referido dictamen se describe al Usuario, como la persona que obtiene monedas virtuales a fin de adquirir bienes o servicios, sin que sean considerados transmisores de moneda virtual.

Un exchanger es la persona dedicada al negocio de cambiar moneda virtual por moneda fiduciaria o por otra moneda virtual. Se diferencia del brooker quienes realizan operaciones de futuro o cobertura (CFD), que tienen como activo subyacente la moneda virtual y que otorgan la posibilidad de vender o comprar el activo en una fecha determinada, a un precio previamente convenido.

El Administrador, es la persona que tiene como actividad la emisión (puesta en circulación) de una moneda virtual, y quién tiene la autoridad para redimir (para retirar de la circulación) dicha moneda virtual. Tanto el administrador como el exchangers pueden transferir monedas virtuales, dependiendo de los hechos y circunstancias específicas. https://www.fincen .gov/resource es/statutes-r egulatio ns/administra tive-rulings/app lication-m oney-services-b usiness-0.

En cuanto a la actividad conocida como minería, los mineros o pool de mineros, son quienes generan los nuevos activos virtuales, mediante un proceso competitivo y descentralizado, mediante el que procesan las transacciones y aseguran la red usando un hardware especializado y reciben criptomonedas a cambio de este servicio. Cuantos más mineros acceden a la red, se incrementa la dificultad para obtener beneficios y los mineros deben procurar una mayor eficiencia para reducir sus costos operativos. https://www.fi ncen.gov/sit es/default/file s/2019-05/F inCEN%20 CVC%20Gu idance%20FINAL. pdf, FinCEN guidance 5.4. CVC Money Transmission Performed by Mining Pools and Cloud Miners

En el caso de los bitcoins se crean a una velocidad predecible y decreciente. El número de bitcoins creados cada año se reduce a la mitad de forma automática a lo largo del tiempo hasta que la emisión se detenga por completo al llegar a los 21 millones https://bitcoin.org/es/faq#mineria,

Cuando ello ocurra, la actividad de minería, respecto de esta moneda, se limitará a la verificación de transacciones que se realicen.

7.2.13. Tipificación en el código penal sobre Fraude a la seguridad social, Robo de planes de beneficios para obreros AFPS.-

Se define el concepto de fraude, distinto del mero incumplimiento de las obligaciones con la Seguridad Social, por cuanto aquel requiere necesariamente la intencionalidad de defraudar, se señalan las causas que lo producen y se estudian los principales sistemas empleados para su cuantificación.

Las nuevas tecnologías de la información y de la comunicación están modificando el funcionamiento de las instituciones aunque aún se encuentran fuertes resistencias a la hora de abordar este cambio trascendental; desde un punto interno se constata una resistencia al cambio Asociación de Ciencias Sociales de Extremadura (ACISE) por parte de ciertos sectores de empleados públicos, no sólo aquellos que desempeñan los puestos más altos, y desde el punto de vista externo, por parte de la ciudadanía, existe todavía una considerable falta de información y adaptación a los procesos telemáticos y, en definitiva, una importante brecha digital fuente : Revista Extremeña de Ciencias Sociales "ALMENARA" nº 10. 2018

8. Capitulo VII

8.1. Conclusiones Y Recomendaciones

8.1.1. Conclusiones.-

Tras el análisis, del desarrollo del **Delito de Estafa Digital** en Bolivia y en otras partes del mundo, y el Estudio de la posibilidad de determinar las características de las variantes ampliamente difundidas en el mundo de este delito informático o (Fraude Informático) que se hace muy complejo y muy difícil de identificar por estar íntimamente vinculado a la Inteligencia artificial, y tras ella el ANONIMATO de los delincuentes, por ser un delito transnacional, cuyas variantes no están tipificadas penalmente, por su dinamismo y velocidad de cambio de procedimientos digitales, sin embargo se ha logrado identificar algunas variantes de Estafa Digital conceptualizando las mismas.

En el contexto de la pandemia COVID-19 se ha acentuado y desarrollado este tipo de delitos, sobre la Estafa Digital, debido a la cuarentena, impuesta por los Estados, como medida precautoria de preservación de salud de la ciudadanía, Paralelamente, a esta situación han proliferado los métodos técnicas digitales, de Este tipo de delito, debido a las necesidades imperiosas de la sociedad para acceder, y satisfacer su economía.

En consecuencia, es necesario, adecuar la normativa, las leyes, decretos supremos, para que regulen, tipifiquen, las variantes que son muchas de los delitos de Estafa Digital o Fraude Digital.

Se propone creando medios de utilización informática como **INFRAESTRUCTURA, INFORMÁTICA DIGITAL, DEPENDIENTE DEL ESTADO PLURINACIONAL DE BOLIVIA.**

Teniendo en cuenta que el Delito Informático, solamente se puede combatir por medios informáticos, con profesionales especializados en cada ámbito, dependiente del Estado.

8.2. Recomendaciones.-

Es cualidad potestativa del Estado Plurinacional de Bolivia, implementar tecnología hardware y software, con el objeto de, proteger a la población de ataques informáticos como ser **la Estafa Digital o Fraude Digital**, ya que solamente una normativa no es suficiente, por ser un delito de carácter transfronterizo.

9. Bibliografía

-ABEL LLUCH, XAVIER y RICHARD GONZÁLEZ (Dir). “Estudios sobre Prueba Penal. Volumen III. Actos de investigación y medios de prueba en el proceso penal: diligencias de instrucción, entrada y registro, intervención de comunicaciones, valoración y revisión de la prueba en vía de recurso”. Ed. La Ley, Madrid, 2013.

-ABEL LLUCH, XAVIER. Nuevas tecnologías e investigación penal en “Estudios sobre Prueba Penal. Volumen III. Actos de investigación y medios de prueba en el proceso penal: diligencias de instrucción, entrada y registro, intervención de comunicaciones, valoración y revisión de la prueba en vía de recurso” (Abel Lluch y Richard González, Dir). Ed. La Ley, Madrid, 2013.

-ADÁN DEL RÍO, CARMEN. “La persecución y sanción de los delitos informáticos”. EGUZKILORE no 20. San Sebastián, Diciembre 2006.

-AGUILAR CÁRCELES, MARTA MARÍA. “Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido”. Revista Criminalidad, vol. 57 no 1, 20015.

-AGUILERA MORALES, MARIEN. “El exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas”. Boletín del Ministerio de Justicia no 2145 Agosto 2012 www.mjusticia.es/bmj

-AGUSTINA SANLLEHÍ, JOSÉ R. “Interrogantes en torno a las diligencias preliminares ante la ciberdelincuencia. Sobre la garantía del derecho a la intimidad en el registro del ordenador (a propósito de la STC 173/2011)”. La ley penal, jurisprudencia no 98-99, Noviembre-diciembre 2012.

-CEDEÑO HERNÁN, M. (COORD.), Nuevas tecnologías y derechos fundamentales en el proceso, Aranzadi, 2017

-DELGADO MARTÍN, J., Investigación tecnológica y prueba digital en todas las jurisdicciones, La Ley 2016

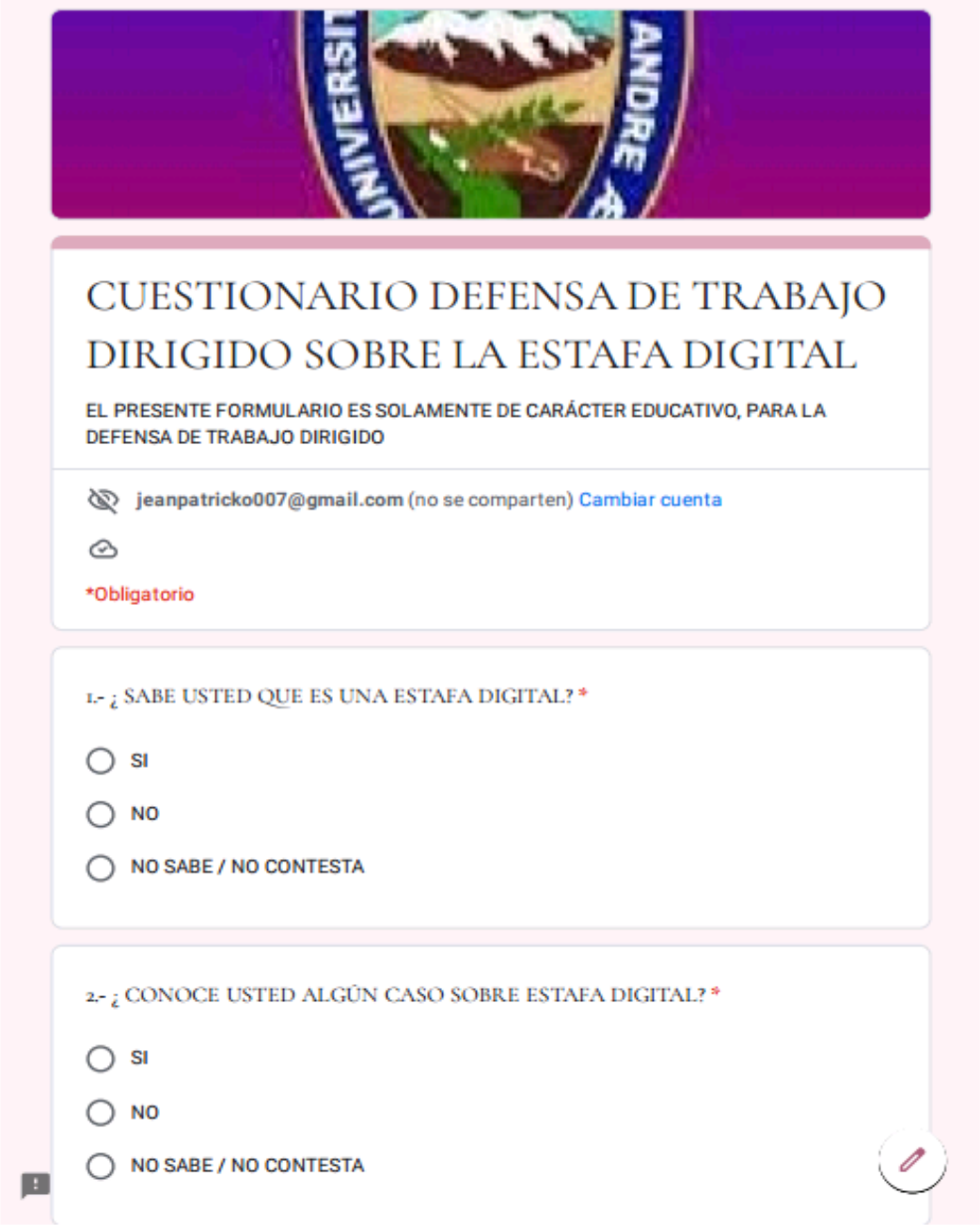
-GONZÁLEZ LÓPEZ, J. J.; PÉREZ GIL, J., The New Technology-Related Investigation Measures in Spanish Criminal Proceedings: An Analysis in the Light of the Right to Data Protection en European Data Protection Law Review 2016 - 2, 242-246

-PÉREZ GIL, J. (Coord.), El proceso penal en la sociedad de la información, La Ley 2011

-RICHARD GONZÁLEZ, M., Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido, La Ley 2017

10. Anexos

Figura nº 1 la encuesta



CUESTIONARIO DEFENSA DE TRABAJO DIRIGIDO SOBRE LA ESTAFA DIGITAL

EL PRESENTE FORMULARIO ES SOLAMENTE DE CARÁCTER EDUCATIVO, PARA LA DEFENSA DE TRABAJO DIRIGIDO

jeanpatricko007@gmail.com (no se comparten) Cambiar cuenta

*Obligatorio

1.- ¿ SABE USTED QUE ES UNA ESTAFA DIGITAL? *

- SI
- NO
- NO SABE / NO CONTESTA

2.- ¿ CONOCE USTED ALGÚN CASO SOBRE ESTAFA DIGITAL? *

- SI
- NO
- NO SABE / NO CONTESTA

3.-¿ HA SIDO USTED VICTIMA DE ESTAFA DIGITAL? *

- ◯ SI
- ◯ NO
- ◯ NO SABE / NO CONTESTA

4.-¿ REALIZA USTED COMPRAS ON LINE? *

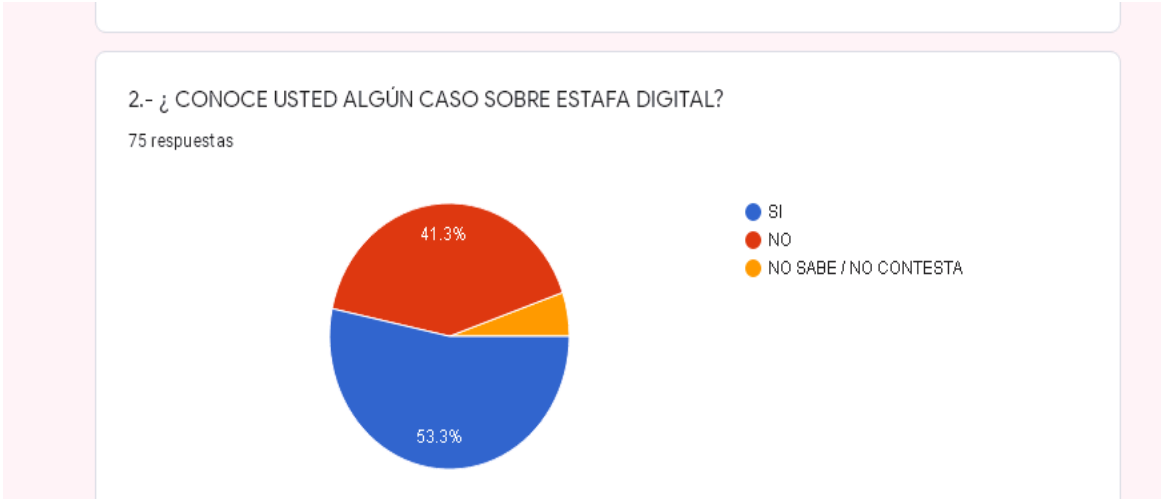
- ◯ SI
- ◯ NO
- ◯ NO SABE / NO CONTESTA

5.- ¿RECIBE USTED INFORMACIÓN SOBRE LA ESTAFA DIGITAL POR PARTE DE SU BANCO O EMPRESA DE SERVICIOS DE INTERNET? *

- ◯ SI
- ◯ NO
- ◯ NO SABE / NO CONTESTA

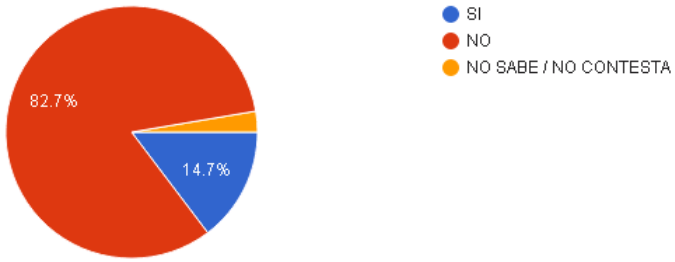
Enviar Borrar formulario

Respuesta al cuestionario, ¿sabe usted que es una estafa digital?



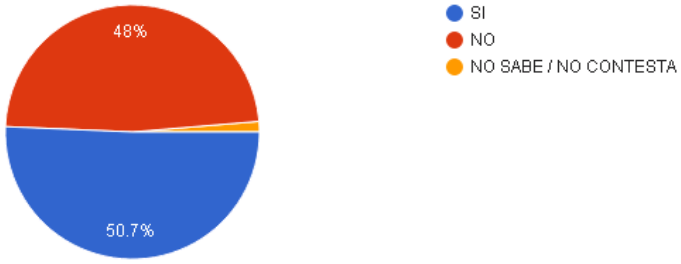
3.-¿ HA SIDO USTED VICTIMA DE ESTAFA DIGITAL?

75 respuestas



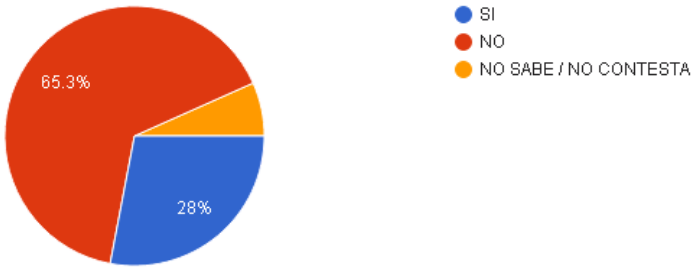
4.-¿ REALIZA USTED COMPRAS ON LINE?

75 respuestas

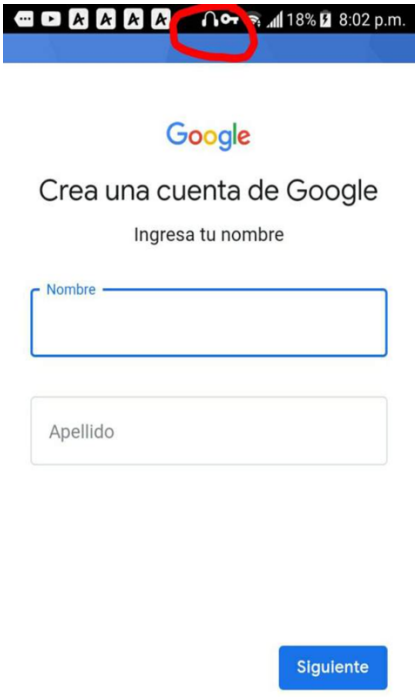


5.- ¿RECIBE USTED INFORMACIÓN SOBRE LA ESTAFA DIGITAL POR PARTE DE SU BANCO O EMPRESA DE SERVICIOS DE INTERNET?

75 respuestas



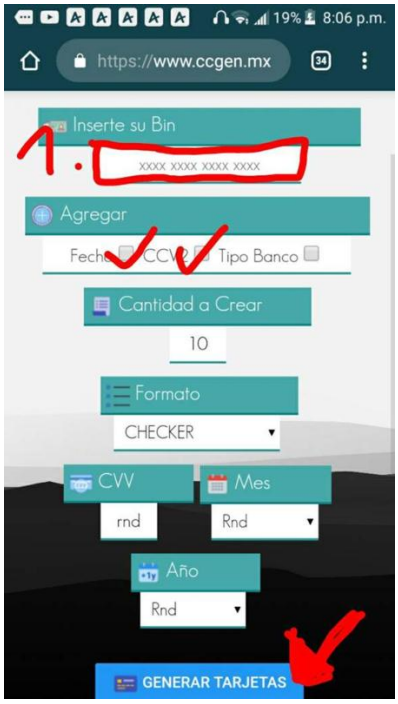
Fotos del caso práctico



Se genera el Bin y guardamos los datos.

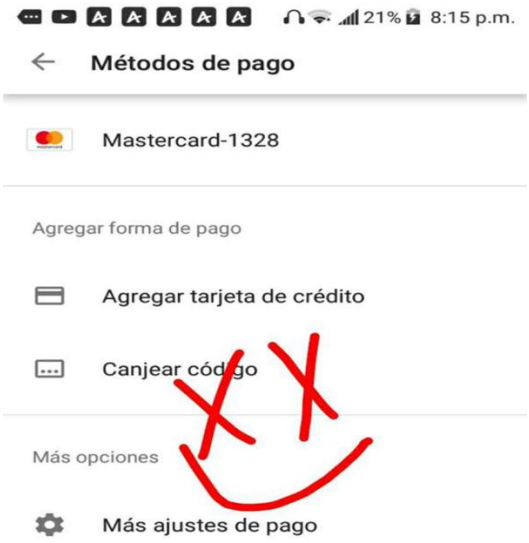
BIN: 527437xxxxxxxxxx
BIN: 545404xxxxxxxxxx
DATE/CVV - rnd
IP: Brazil
CPF: 133.267.246-91
Phone Number: 612648xxxx
Dirección 1 : Street Jeff xxxx
Dirección 2 : (Vacío)
Postal: 41500290
BARRIO/NEIGHBORHOOD: SÃO CRISTÓVÃO
ESTADO/STATE: BAHIA
CIUDAD/CITY : SALVADOR

Las X se sustituyen por números al azar, como se ve se tiene un bin y varios datos que ayudaran dentro de poco a generar el Bin, ingresando a cualquier página de cc gen en este caso será ccgen.mx



Se marca las opciones de fecha y cvv, la de banco no es obligatoria y después se pondrá en la casilla de bin 527437XXXXXXXXX y se asignara a generar después se guarda las ccs en algún lugar

Después se ingresa a la cuenta ya en la play store y se da los pagos.



Otro método de obtención de Bins para conseguir entradas en Cinepolis y para HBO se ingresa a Cinepolis.com y se crea una cuenta nueva con un correo electrónico de Outlook https://www. Cinepolisklic.com se registra con el correo Outlook se agrega un método de pago se genera la tarjeta y se coloca datos.

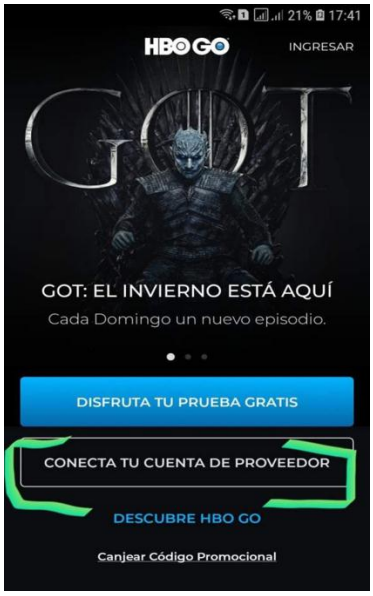
528843912580XXXX

02/22

Ccv 000 a 485

5470466018XXXXX

Todo generado el método de pago en HBO GO o en cinepolis klic y se compra la suscripción, si no entra a la primera se vuelve a comprar y solo se llena la cvv y listo!



Por último se confirma por el correo electrónico Outlook o Hotmail cuando llegue la verificación, se abre el enlace en modo escritorio y a disfrutar.