UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARREA DE DERECHO

INSTITUTO DE INVESTIGACIONES Y SEMINARIOS

TESIS DE GRADO

"INSERCIÓN DE LA FIGURA PENAL DE SUPLANTACIÓN DE IDENTIDAD COMO DELITO INFORMÁTICO EN EL ART. 363 DEL CÓDIGO PENAL"

(Tesis para optar al grado Académico de Licenciatura de Derecho)

POSTULANTE: Salvador Eddy Gutierrez Alejo

TUTOR: Dr. Marcelo Fernández Iraola

LA PAZ – BOLIVIA
2023

DEDICATORIA

Dedicó este trabajo principalmente a Dios, por darme vida, haberme guiado y acompañado a lo largo de este camino para culminar con satisfacción un escalón más en mi vida profesional.

A mi madre, que con su paciencia dedicación, esfuerzo y ejemplo me brinda la fortaleza necesaria, para poder cumplir las metas que me propongo.

AGRADECIMIENTO

A la Universidad Mayor de San Andrés, alma mater de mi formación y a su plantel docente que han sido parte de mi camino universitario, a todos ellos les quiero agradecer por transmitirme los conocimientos necesarios para poder estar aquí hoy.

Al Dr. Marcelo Fernández Iraola, por guiarme en la elaboración de la presente tesis, sin su dedicación, paciencia, palabras y apoyo no hubiese logrado llegar a esta instancia tan anhelada. Gracias por su guía y todos sus consejos, los llevaré grabados para siempre en la memoria en mi futuro profesional.

RESUMEN- ABSTRAC

La presente tesis Titulado: “INSERCIÓN DE LA FIGURA PENAL DE SUPLANTACIÓN DE IDENTIDAD COMO DELITO INFORMÁTICO EN EL ART. 363 DEL CÓDIGO PENAL”, la misma es una investigación a nivel doctrinario con el fin de demostrar la necesidad de incorporar la tipificación como nuevo delito de tipo penal, la suplantación de identidad informática en nuestra actual legislación Penal.

A través del avance tecnológico, se explica el constante desarrollo de la de la misma y la aparición de vacíos legales dentro de nuestra legislación penal con relación a los delitos informáticos, y los artículos que hacen referencia a este tipo de ilícitos, denominados delitos informáticos en el Código Penal.

Es preciso entonces una regulación efectiva e incorporar en nuestro Código Penal la suplantación de identidad informática debido que existe en nuestro país la necesidad de incorporar nuevos tipos penales para sancionar a aquellos delincuentes que cometen delitos informáticos ya que actualmente no contamos con legislación específica para tratar este tipo de delitos, también hacer constar que la existencia de la Suplantación de Identidad Informática como delito informático afecta directamente a un derecho fundamental que es de la intimidad y privacidad.

Esta tesis es producto de una investigación cualitativa, descriptiva realizada a través de la consulta doctrinaria, legislación vigente nacional y comparada y de las opiniones de profesionales abogados, estudiantes, así como Autoridades del órgano Judicial, concluyendo entonces que existen los necesarios y suficientes fundamentos para la incorporación de la Suplantación de Identidad Informática como nuevo tipo Penal dentro de nuestra Legislación Penal.

ÍNDICE GENERAL

INTRODUCCIÓN

La presente tesis surge en base a la observación referida al desarrollo de las Tecnologías de la Información y de la Comunicación (Tic´s) ya que, en los últimos 30 años, el Internet se ha posicionado como una de las herramientas más útiles para la sociedad, tanto en entidades bancarias o diferentes instituciones públicas y privadas o simplemente en las Redes Sociales en que los individuos pueden interactuar entre ellos de forma más amplia sin tener en cuenta las barreras de tiempo y espacio.

La autonomía que se le ofrece al usuario en el mundo virtual, ha permitido que éste pueda decidir entre múltiples opciones para representarse en el ciberespacio, con la libertad incluso de crear una falsa identidad o forma de identificación; en algún caso esta “libertad”, sumada a conocimientos en informática y manejo de medios digitales , mal utilizada, permite, ocupar identidades ajenas, promoviendo la aparición de nuevos delitos denominados, ahora, informáticos.

Ahora la suplantación de identidad también denominada *phishing*, consiste en un ataque informático que consiste en la obtención de información confidencial referente a la identidad de una persona que se constituye en víctima, mediante el uso solicitudes engañosas publicadas en medios digitales, que en muchos casos es utilizada para generar fraudes patrimoniales y extrapatrimoniales. Este tipo de delitos se cometen en contra de personas comunes, pero también, se han dado casos donde, las víctimas son organizaciones o empresas, el pissihing está referido a la suplantación o robo de identidad generada por el uso de sistemas informáticos, la aplicación deficiente de medidas de seguridad en relación a correo electrónico, páginas web o navegadores de internet o simplemente el uso del engaño para que el usuario entregue, sin saberlo, información confidencial a terceros (Belisario, 2018), esta actividad delictiva no está sancionada de manera formal en el ordenamiento jurídico boliviano.

Por lo mencionado, es necesario proponer un Anteproyecto de Ley que modifique un artículo del Código Penal boliviano a fin de sancionar la suplantación de identidad realizada a través de Internet y redes sociales, así como de las Tic´s; esto, con el propósito de proteger la seguridad de las personas que usan los medios digitales como un elemento de comunicación, distracción, trabajo y negocio.

La presente tesis denominada “Inserción de la Figura Penal de suplantación de identidad como Delito Informático en el Art. 363 del Código Penal” que pretende proteger la identidad de las personas en el momento en que usen los medios digitales como elementos de trabajo, comunicación y diversión. La investigación propuesta se ha planteado desde la perspectiva analítica, exegética de carácter inductivo y con un enfoque cuali-cuantitativo.

Este documento se estructura de la siguiente manera:

1. ENUNCIADO DEL TEMA DE LA TESIS

“INSERCIÓN DE LA FIGURA PENAL DE SUPLANTACIÓN DE IDENTIDAD COMO DELITO INFORMÁTICO EN EL ART. 363 DEL CÓDIGO PENAL”

2. IDENTIFICACIÓN DEL PROBLEMA

La presente tesis aborda una problemática que va a la par de los avances tecnológicos que han permitido el acortamiento de tiempo y distancia entre la comunicación de las personas, en tal sentido el incremento del uso de medios digitales ha revolucionado la forma de relacionarse de las sociedades y ha logrado generar muchos beneficios de flujo de información, de comunicación y de comercialización, pero también ha generado una serie de facilidades para la comisión de delitos que actualmente se denominan informáticos que representan una amenaza constante para la seguridad de quienes interactúan en línea o conectados a una red de internet. Estos delitos se han convertido en una preocupación cada vez mayor debido al aumento de la actividad de interacción que genera la conexión en red de las instituciones, organizaciones y familias enteras y la dependencia de la tecnología en las actividades cotidianas de la vida humana.

Bolivia a pesar de sus avances en Materia Penal posee algunos vacíos jurídicos como por ejemplo la no tipificación del robo y/o suplantación de identidad por medio del uso de sistemas informáticos, el Estado no ha generado la normativa que pueda regular el relacionamiento social mediado por tecnología. Actualmente el uso de medios de información y comunicación digitales ha proporcionado, a personas cuyo comportamiento es delictivo, nuevas oportunidades para cometer delitos informáticos aprovechando la predisponibilidad a la entrega de datos personales de los usuarios comunes que se conectan a una determinada plataforma informática. Existen tantos datos

personales y financieros almacenados en línea que se acumulan por el uso de aplicaciones y/o actividades comerciales realizadas, que, existe una predisponibilidad de los delincuentes para acceder a esta información de forma ilegal. El robo de identidad, el fraude con tarjetas de crédito, el acceso no autorizado a cuentas bancarias y el espionaje cibernético son solo algunos ejemplos de delitos informáticos que se han vuelto más comunes debido al crecimiento del uso de medios digitales.

Como se ha mencionado antes, junto a las innegables ventajas que presenta la era digital que actualmente se vive en Bolivia y el mundo, comienzan a aparecer algunos aspectos negativos producto de la criminalidad informática o los delitos informáticos, de ahí nace el phishing que se refiere a una técnica utilizada por los delitos informáticos para obtener de manera ilegal la información confidencial, como contraseñas, datos confidenciales, fotografías de perfil o datos bancarios, haciéndose pasar por una entidad o persona legítima, en esta técnica delictiva los delincuentes envían mensajes de correo electrónico, mensajes de texto o publicaciones falsificados que parecen provenir de una organización confiable como un banco o una empresa reconocida y solicitan a los usuarios que proporcionen información personal o realicen acciones que comprometan su seguridad pidiendo la entrega de contraseñas y datos de uso personal que luego son utilizados de manera fraudulenta en contra del propietario de los datos proporcionados.

Ahora, puntualmente el phishing o la suplantación de identidad como delito informático se manifiesta cuando se realiza una actividad que, basada en la ingeniería social y la manipulación psicológica, personas con intencionalidad y premeditación diseñan y envían mensajes que utilizando información convincente induce a los usuarios comunes de los medios digitales a actuar de acuerdo con las solicitudes fraudulentas. Esto puede implicar hacer clic en enlaces maliciosos, proporcionar información confidencial o incluso transferir fondos a cuentas controladas por los delincuentes motivados por este accionar delictivo.

La comisión de este tipo de delitos genera en los individuos y las organizaciones afectadas consecuencias complejas, los usuarios que han otorgado una contraseña sin darse cuenta pueden perder acceso a sus cuentas bancarias, sufrir robo de identidad, ser víctimas de extorsión o enfrentar daños financieros significativos. Además, las empresas pueden experimentar pérdida de datos, daño a su reputación y consecuencias legales, el phishing no solo afecta a las personas involucradas directamente, sino que también tiene un impacto más amplio en la confianza de los usuarios en línea y en la seguridad de las transacciones digitales, las mismas que se ven afectadas.

En consecuencia y ante la inexistencia de legislación específica que regules estos actos ilícitos en Bolivia y en muchos países no existen sanciones especificas contra la suplantación de identidad o phishing, este extremo responde a varias razones; en primera instancia, la naturaleza evolutiva y destaca los delitos informáticos como la suplantación de identidad hace que sea difícil para las legislaciones mantenerse al día y adaptarse rápidamente a estas nuevas formas de delincuencia, así en Bolivia esta actividad delictiva no ha sido aún abordada.

Además, la falta de cooperación y coordinación internacional en la lucha contra los delitos informáticos puede obstaculizar los esfuerzos para sancionar este tipo de actividad delictiva , esto, en la medida de que, los delincuentes pueden operar desde diferentes jurisdicciones y utilizar técnicas para ocultar su identidad y ubicación, lo que dificulta su identificación y correspondiente sanción.

En tal sentido el presente estudio se centra en el análisis de la “SUPLANTACIÓN DE IDENTIDAD COMO DELITO INFORMÁTICO” que aun constituye un vacío jurídico en la legislación nacional ya que en Bolivia los delitos informáticos son tratados como delitos comunes, hasta ahora, se plantea entonces incluir en el Código Penal la figura de la suplantación de identidad como un delito que atenta contra la integridad de las y los usuarios de medios digitales de información y comunicación en Bolivia.

3. PROBLEMATIZACIÓN

Los aspectos puntuales ya señalados, permiten formular el problema de investigación de la siguiente manera:

La falta de una regulación jurídica no sanciona la Suplantación de Identidad como delito Informático ya que dentro el Código Penal Boliviano no se encuentra tipificado este accionar como delito Informático generando indefensión para aquellos ciudadanos que realizan actividades cotidianas de trabajo, relacionamiento comercial o social en medios digitales de información y comunicación.

4. DELIMITACIÓN DEL TEMA DE LA TESIS

4.1. DELIMITACIÓN TEMÁTICA.

La presente tesis se enmarca en el análisis Jurídico Social, de la problemática de la comisión y aparición de nuevos delitos denominados informáticos y como esta afecta a gran mayoría de la sociedad que están inmersa en la utilización de las TIC´s.

4.2. DELIMITACIÓN TEMPORAL

La toma de datos que hacen al análisis de la temática abordada en la presente investigación considera el periodo comprendido entre el año 2016 a la fecha, considerando como inicio el año 2016 puesto que ese ha sido el año en el que, según la revista digital “Economy”, en Bolivia se ha llegado a un total de 5,57 millones de ciudadanos suscritos a la Red social Facebook, considerada una de las redes de interacción digital más grande del mundo (Rosado, 2020).

4.3. DELIMITACIÓN ESPACIAL

La propuesta resultante de la presente investigación pretende tener un ámbito de aplicación nacional, pero a efectos de recolección de datos, la misma se circunscribe a tomar en cuenta como campo de estudio y de investigación la ciudad de La Paz, Bolivia.

5. FUNDAMENTACIÓN E IMPORTANCIA DEL TEMA DE LA TESIS

En los últimos 30 años, la Internet se ha posicionado como una de las herramientas más útiles para la sociedad, tanto así que hoy en día no se concibe la vida sin este medio. En la actualidad vive su apogeo, con las redes sociales como su máxima expresión, configurándose como un mundo propio, en el que los individuos pueden desarrollar de forma más amplia casi todos los aspectos de su vida, razón por la cual los mismos buscan construir la propia identidad dentro de estas plataformas, para así autodefinirse en este nuevo plano y poder ser reconocidos por los demás.

La autonomía que se le ofrece al usuario en el mundo virtual, ha permitido que éste pueda decidir entre múltiples opciones para representarse en el ciberespacio, ya sea extendiendo su propia identidad, creando una falsa, o bien, ocupando una ajena.

Respecto a este último punto se enfoca nuestro análisis, en cuanto el ilícito de usurpación de identidad ha encontrado un nuevo nicho para perpetrarse, creando nuevos desafíos que se ven agravados por el avance tecnológico que no hace más que moverse a pasos agigantados. En este sentido, el objetivo de la tesis es determinar, si el Anteproyecto de Ley que “modifica un artículo del Código Penal Boliviano, es pertinente, para sancionar la suplantación de identidad realizada a través de Internet y redes sociales, así como de las NTIC´S, ya que estos ocasionan daños a terceros, así también identificar si es necesario, o si es

suficiente que el artículo 363 del mismo cuerpo normativo, sea el adecuado para tipificar el delito de usurpación de identidad, todo ello con el propósito de proteger la identidad de aquellas personas que se ven afectadas por el uso indebido y no autorizado de la misma por terceros ajenos.

6. OBJETIVOS DEL TEMA DE LA TESIS

6.1. OBJETIVO GENERAL

Diseñar un anteproyecto de ley que modifique el Artículo 363 del Código penal boliviano que defina la figura penal y la sanción de la suplantación de identidad como delito informático para proteger la integridad personal, social y económica de los ciudadanos bolivianos

6.2. OBJETIVOS ESPECÍFICOS

- Establecer los parámetros teórico normativos que regulan el derecho a la identidad real y la identidad virtual
- Analizar las bases jurídicas que definen la figura penal de la suplantación de identidad como delito informático
- Determinar el tratamiento jurídico del delito de la suplantación de identidad en las sociedades de países colindantes con Bolivia
- Estudiar las implicancias sociales y jurídicas que causa la suplantación de identidad como delito informático en la población boliviana

7. HIPÓTESIS DE TRABAJO

La modificación del Artículo 363 del Código Penal Boliviano que defina la figura penal y la sanción de la suplantación de identidad como delito informático,

permitirá proteger la integridad personal, social y económica de los ciudadanos bolivianos

7.1. Variable Independiente (Causa)

Modificación del Artículo 363 del Código penal boliviano que defina la figura penal y la sanción de la suplantación de identidad como delito informático

7.2. Variable Dependiente (Efecto)

Proteger la integridad personal, social y económica de los ciudadanos bolivianos

7.3. Nexo Lógico

Permitirá

8. MÉTODOS DE INVESTIGACIÓN

8.1. Método General

La presente investigación utilizará como método general la investigación analítica que es el estudio que tiene como objetivo analizar un evento o fenómeno y comprenderlo en términos de sus aspectos menos evidentes. Analizar significa desintegrar o descomponer una totalidad en todas sus partes (Hernandez y otros, 2014). La aplicación de este método permitirá descomponer en partes de estudio y analizar por separado la suplantación de identidad, la ingeniería social, el delito informático y la normativa penal vigente en Bolivia

Así mismo la indagación utilizará el método exegético**,** por el manejo de diferentes leyes que regulan el comportamiento ciudadano respecto de las actividades guiadas por sistemas informáticos, esto en la medida de que se entiende por investigación exegética a aquella que se utiliza en el estudio de los textos legales y que se centra en la forma en la que fue redactada la ley o

regulación por parte del legislador. Se estudia mediante el análisis de las reglas gramaticales y del lenguaje para logra una interpretación específica de la norma (Vargas Flores, 2012).

8.2. Métodos Específicos

La investigación en el campo jurídico utilizará el método teleológico**,** que tiene por finalidad encontrar el interés jurídicamente protegido, debido a que cada norma jurídica protege un interés, en consecuencia, este método permite determinar el interés que protege una determinada norma jurídica a proponer (Vargas Flores, 2012)

Este método permite entonces analizar cómo generar la protección de las personas que utilizan medios digitales para realizar actividades de trabajo, comunicación, comercialización, transmisión de información y/o actividades recreativas, precautelado que no sean víctimas de una suplantación de identidad informática.

Al ser una investigación orientada al área penal del derecho, también, se utilizará el método dogmático jurídico, que se refiere al método de estudio e investigación cuyo objeto de aplicación es el análisis de la norma. La característica de este método jurídico es la interpretación de la ley. En la ciencia penal se expresa la dogmática como sistema, aspirando a establecer las bases para una administración de justicia igualitaria y justa, ya que sólo la comprensión de las conexiones internas del derecho libera a su aplicación de la interpretación (Vargas Flores, 2012).

8.3. Diseño de Investigación

De acuerdo con las características del estudio realizado en la presente investigación se utilizó un diseño no experimental, transversal. El estudio no experimental es aquel que: ”se realiza sin manipular deliberadamente las variables de estudio, es decir, se trata de investigaciones donde no se hace variar

intencionalmente una variable. La investigación no experimental es aquella que permite observar fenómenos tal y como se dan en su contexto natural, para después analizarlos" (Hernández y otros, 2014).

Se determina las características no experimentales del estudio, dado que se trata de manejar la información obtenida respecto al tema de análisis sin modificarla o alterarla en ningún momento. Por otro lado, se utiliza un estudio de diseño transversal que es aquel que se refiere a la recolección de datos en un solo momento de tiempo, en un momento único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado, es como tomar una fotografía de algo que sucede (Hernández y otros, 2014).

Este hecho, refiere que el estudio, levantará datos en un solo momento, sin necesidad de tener que corroborar los datos respecto de otros tomados en otra etapa o tiempo. Es decir que el estudio debe reflejar los datos contemplados en el momento del examen o evaluación, sin esperar que estos se modifiquen con el paso del tiempo, los datos del estudio son referidos a la apreciación de la ciudadanía respecto de los delitos informáticos, la suplantación de identidad y la indefensión en la que se encuentran en la actualidad.

8.4. Técnicas a utilizar en la tesis

La técnica de recolección de datos para el análisis de los resultados de esta investigación, son las siguientes:

Encuesta

La encuesta es una técnica de adquisición de información, mediante un cuestionario previamente elaborado, a través del cual se puede conocer la opinión o valoración del sujeto seleccionado en una muestra sobre un asunto dado, en el presente estudio esta encuesta es aplicada a los ciudadanos residentes de la ciudad de La Paz, mayores de 18 años que tengan algún tipo de conexión o

interacción por medios digitales y que se encuentran en indefensión ante la no existencia de la identificación del delito de la suplantación de identidad informática

Revisión Documental

La revisión de documentos permitirá conocer los alcances, las limitaciones, las repercusiones de los procesos de la investigación respecto al tratamiento de los delitos informáticos en el ordenamiento jurídico, también permite la fundamentación teórica que hace a la materia de estudio y sustenta la presente investigación.

CAPITULO I

MARCO HISTÓRICO

1.1. MARCO HISTÓRICO

Si bien el internet no fue implementada recientemente, cabe mencionar que en los últimos diez años, las redes sociales se han impuesto como una tendencia a nivel mundial, por lo que se le ha dado una autonomía total al usuario, por lo que en consecuencia se tiene que en los últimos años indicados se han cometido delitos llamados “cibernéticos”, a consecuencia de la libertad con la que cualquier persona puede utilizar las redes sociales, y es así que hacerse pasar por otra persona mediante el robo de datos es un problema que va en aumento, sobre todo por el impulso de internet y las redes sociales. De hecho, esta situación ha incrementado en un 178% en los dos últimos años, según datos de la Oficina de Seguridad del Internauta (OSI) de Estados Unidos (OSI, 2022).

Así mismo se sabe que el Internet cuenta con múltiples beneficios y ventajas, pero también presenta peligros ocultos que pueden poner en jaque hasta a la multinacional más preparada. Uno de los problemas que pueden aparecer es la pérdida de datos, que alguien nos robe información o que suplante nuestra identidad. Basta con que un delincuente acceda a ellos para usurpar la identidad de un tercero y vaciar la cuenta bancaria. Con un simple número de documento de identidad o con los datos personales adecuados, un defraudador puede solicitar préstamos, contratar tarjetas de crédito, hacer transferencias, realizar compras financiadas o hasta organizar un matrimonio en nombre de su víctima (Borja, 2021)

Por estos tipos de incidentes, los ataques con troyanos (un tipo de malware que permite al hacker acceder de forma remota al dispositivo), son los más numerosos, y están presentes en más de la mitad de los ataques; seguidos de la explotación de vulnerabilidades del sistema (17,6%); la infiltración de código malicioso (9,6%), y los gusanos (5,3%). El phishing (fraude informático mediante la suplantación de identidad) pese a sólo representar el 0,9% de los ataques, ocasionó pérdidas el año pasado por valor de 60 millones de euros (OSI, 2022).

Uno de los objetivos más comunes del robo de datos personales es la contratación de servicios o la compra de ciertos objetos dando el número de cuenta o la tarjeta de crédito de una tercera persona, que puede acabar incluso en un registro de morosos al rechazar las facturas por algo que realmente ni ha comprado ni está utilizando.

Sin embargo, el gran problema que existe en la actualidad en cuanto a la ciber-seguridad no es el hecho de que alguien pueda robar nuestra información, sino que nosotros mismos se la facilitemos a terceros sin ser conscientes de ello. Cada vez que nos conectamos a la red y nos registramos en una página, nos abrimos una cuenta en una red social o instalamos una aplicación estamos cediendo información a las compañías que gestionan ese software (OSI, 2022).

Además de este gran talón de Aquiles, en general el grueso de las empresas también peca de una mala organización a nivel tecnológico que provoca que su seguridad esté muy debilitada y sus datos queden a merced de los ciber-ataques. El principal motivo de estos ciber-ataques es la obtención de un beneficio económico por parte de los delincuentes, pero también es lograr accesos no autorizados a cuentas de directivos o altos cargos de las empresas con la finalidad de robar información (BBVA, 2020),a todo ello se está expuesto con la falta de seguridad en el manejo informático de datos.

En términos de seguridad, lo mejor es pensar que una empresa es como un ser humano. Tomar medidas de precaución no significa que no puedas enfermar, pero desde luego sí potenciará que no seas propenso a hacerlo. Operar en Internet es lo mismo, no existe una seguridad total pero sí se pueden tomar ciertas medidas para proteger, dentro de lo posible, la integridad de tu empresa frente a los hackers (BBVA, 2020).

1.2. LA EVOLUCIÓN DEL DERECHO PENAL Y LOS DELITOS INFORMÁTICOS.

Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados. En la actualidad el delito informático, o crimen electrónico, es el término genérico empleado para denominar aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivos destruir y dañar ordenadores, medios electrónicos y redes de Internet (Rendon, 2012).

Es posible afirmar, sin embargo, que las categorías que definen un delito informático son aún mayores y complejas, dado que pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados.

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de datos), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial, entre otros (Rendon, 2012).

Un ejemplo común es cuando una persona comienza a robar información de websites o causa daños a redes o servidores. Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra en forma digital y el daño, aunque real no tiene consecuencias físicas distintas a los daños causados sobre los ordenadores o servidores

En algunos sistemas judiciales la propiedad intangible no puede ser robada y el daño debe ser visible. Un ordenador puede ser fuente de pruebas y, aunque el ordenador no haya sido directamente utilizado para cometer el crimen, es un excelente artefacto que guarda los registros, especialmente en su posibilidad de codificar los datos. Esto ha hecho que los datos codificados de un ordenador o servidor tengan el valor absoluto de prueba ante cualquier corte del mundo (Calderon, 2021).

En el ámbito internacional existente, dada la necesidad creada por su proliferación, los diferentes países suelen tener policía especializada en la investigación de estos complejos delitos, que, al ser cometidos a través de internet, en un gran porcentaje de casos excede las fronteras de un único país complicando su esclarecimiento viéndose dificultado por la diferente legislación de cada Estado o simplemente la inexistencia de ésta (Borja, 2021).

1.3. CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

Pasemos ahora a definir las características del delito informático, quién mejor los establece es el jurista mexicano Julio Téllez Valdés quién desarrolla en forma específica las siguientes características (Téllez, 2005):

1	Son conductas criminales de cuello blanco, porque sólo un determinado número de personas con ciertos conocimientos técnicos puede llegar a cometerlas.
2	Son acciones ocupacionales, porque en muchas veces se realizan cuando el sujeto se halla trabajando.
3	Son acciones de oportunidad, porque se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
4	Provocan serias pérdidas económicas.
5	Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

6	Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
7	Son muy sofisticados.
8	Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
9	En su mayoría son imprudencias y no necesariamente se cometen con intención.
10	Ofrecen facilidades para su comisión los menores de edad.
11	Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

1.4 LA SEGURIDAD INFORMÁTICA:

Este concepto abarca todos aquellos pasos y métodos para la protección de datos personales, equipos informáticos, claves personales, protocolos de seguridad, ya que para un usuario le afecta tanto perder información como el propio equipo donde se encuentra la misma o incluso la protección de otros bienes dentro de su patrimonio. Durante los años se ha venido perfeccionando todo lo relacionado a los sistemas de computación, adecuándose máquinas con mayor capacidad, con mayores funciones, más rápidas, más pequeñas, con mayor duración, etc. Sin olvidarlas diversas formas para recibir, procesar y transmitir la información, creándose para todo ello diversos sistemas de seguridad. Ahora existen diversos sistemas de cómputo que guardan la información en altos índices de seguridad a lo que se le ha llamado “encriptar la información” desgraciadamente los diversos delincuentes informáticos a los que hemos hecho referencia se han encontrado pasos adelante para poder cometer sus conductas delictivas (Kaspersky, 2020).

CAPITULO II

MARCO CONCEPTUAL

MARCO CONCEPTUAL

2.1. ¿QUÉ ES LA IDENTIDAD PERSONAL?

Es la percepción individual que una persona tiene sobre sí misma, es la conciencia de existir. Son una serie de datos que se adquieren a lo largo de la vida, capaces de moldear el patrón de conducta y la personalidad. Su desarrollo comienza cuando el niño, ya consciente tanto de la presencia de otros como la suya en el mundo, paso a paso, procesa el papel que representa la sociedad (Fricke, 2010).

2.2. ¿QUÉ ES LA SUPLANTACIÓN DE IDENTIDAD?

Se entiende como aquella acción por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal, como pueden ser pedir un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o realizar ataques contra terceras personas (Rimber, 2018).

Esta acción es cada vez más habitual en las redes sociales, en las que una persona se hace con fotografías y datos de otra y crea perfiles en su nombre, desde los cuales realiza actividades tales como insultos a terceras personas o incluso llegan a apropiarse de datos personales debido a la poca seguridad de la que gozan algunas APP móviles o cuentas de correo.

Según el tipo de *suplantación* que se realice conlleva una u otra pena, así, cuando la suplantación de identidad consiste únicamente en la apertura o registro de un perfil sin que en él se den datos personales, la opción que tiene el suplantado es hablar con el portal web, foro o red social para que sean sus administradores quienes eliminen el perfil falso. Es decir, el hecho de utilizar sólo el nombre, sin imágenes, no se considera delito (Rimber, 2018).

El robo, hurto o apropiación de la identidad de una persona se utiliza, siempre en perjuicio de la víctima, pues el acceso es ilegal y sin permiso. La falta de protección al consumidor de servicios de comunicación mediante dispositivos electrónicos vulnera indiscriminadamente a los usuarios de cualquier dispositivo electrónico (Téllez, 2005)

Ahora en este entendido se puede entender a la suplantación de identidad como un delito siempre que el infractor haya aprovechado de todas las características que dan identidad para cometer un acto en favor suyo, pero para que se configure como tal, quien ha usurpado la identidad debe realizar acciones que solo el propietario puede realizar sin consentimiento del titular.

2.3. DERECHO INFORMÁTICO

Se caracterizan por el constante cambio, el que cada día sorprende más por su rapidez y profunda incidencia en el desarrollo de patrones de conducta social, creando entre las personas nuevos modos de interacción. Sin embargo, no se está únicamente en presencia del progreso científico o tecnológico, sino que el cambio involucra las creencias, las actitudes psicológicas, el ámbito económico y político; en suma, la forma de convivir en el mundo. Es decir, se está viviendo un verdadero cambio social que modifica irreversiblemente los modos de conducta en sociedad.

“Sin lugar a dudas, estos cambios sociales profundos se tienen que reflejar a través de modificaciones serias en el ordenamiento jurídico, como sucede por ejemplo, con el surgimiento de la legislación medioambiental o las normas que rigen a las tecnologías de la información. Ante ello, la rama del Derecho no puede negarse a la capacidad de interpretar mejor las necesidades humanas y de adaptarse en forma más perfecta a lo que de él se requiere para el bien común, la paz, la justicia y el progreso” (Núñez Ponce, 2007)

La revolución tecnológica ha redimensionado las relaciones entre los hombres. Se está ante una sociedad donde las tecnologías de la información han

llegado a ser la figura representativa de la cultura, hasta el punto de que para designar el marco de la convivencia se alude reiteradamente a la expresión *Sociedad de la Información* (Herrera, 2004)

2.4. DEFINICIÓN DE DELITOS INFORMÁTICOS

Dar un concepto sobre delitos informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de *delitos* en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión delitos informáticos, este consignada en los códigos penales, lo cual en Bolivia al igual que en muchos otros, no ha sido objeto de identificación aún; solo con excepción del estado de Sinaloa que ya incluyó esta modalidad (Herrera, 2004).

Actualmente, se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar estos malos usos en el Internet, y el objetivo de este trabajo de investigación es sugerir la inclusión dentro del Código Penal Boliviano, un proyecto de ley que tipifique y penalicé la suplantación y/o robo de identidad en el Artículo 363 de nuestro Código Penal, porque cada día aparecen nuevos métodos de vulneración de los sistemas, aparte de los fraudes y todo el mal uso que se está dando al Internet por lo tanto se hace necesario que también la leyes se deben mover con la tecnología, para mantener una actualización porque tanto, en el campo de la informática así como el derecho todo cambia continuamente.

2.5. DEFINICIÓN DE INTERNET

Los autores consultados, señalan que el Protocolo de Internet (IP) y el Protocolo de Control de Transmisión (TCP) fueron desarrollados inicialmente como una idea en 1969, posteriormente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero estadounidense Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de

Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPANET) que conectaba redes de ordenadores de varias universidades y laboratorios de investigación en Estados Unidos. La World Wide Web fue desarrollada en 1989 por el informático británico Timothy Berners-Lee para Organización Europea para la Investigación Nuclear, más conocida como CERN (Atheniense, 2012)

2.6. LAS SUPLANTACIONES INFORMÁTICAS

2.6.1. Phising

"Phishing es un término informático utilizado para denominar el fraude por suplantación de identidad, una técnica de ingeniería social. El origen de la palabra phishing se dice que proviene de la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas); sin embargo, esta explicación es muy probable que sea posterior al propio término. El término phishing procede de la palabra inglesa "fishing" (pesca) haciendo alusión a "picar el anzuelo" (Rodríguez, 2012).

Este término se acuñó por primera vez en 1996, en los casos de intento de apropiación de cuentas de AOL, a pesar de que se había iniciado varios años antes. Se trataba de envío de mensajes instantáneos haciéndose pasar por empleados de AOL, solicitando contraseñas. AOL tomó medidas en el año 1995, y reforzó las mismas en 1997. Las personas que realizan el fraude se denominan phishers. Su objetivo es la obtención de información personal confidencial de las víctimas, ya sean cuentas bancarias, contraseñas, números de tarjetas de crédito, etcétera (Rodríguez, 2012).

El phisher actúa de varias formas distintas para conseguir la información: mediante el envío de mensajes de correo electrónico fraudulentos, mensajería instantánea o mediante la utilización de falsos sitios web. En este último caso podemos enmarcar los casos de suplantación de páginas web de entidades bancarias muy utilizados actualmente.

Generalmente en el caso de los correos, el envío masivo, pese a ser buenas falsificaciones y ser aparentemente veraces, no suele ser muy efectivo pues llega a personas que no tienen ninguna relación con la entidad que es falsificada. Por ello, otra forma más efectiva es relacionar por cualquier método de ingeniería o investigación a cada posible víctima con una entidad que será falsificada, ya sea cliente o empleado. En este caso la probabilidad de éxito es mucho mayor, pues está dirigida y es más creíble. Este caso se denomina spear phishing, investigación a cada posible víctima con una entidad que será falsificada, ya sea cliente o empleado. En este caso la probabilidad de éxito es mucho mayor, pues está dirigida y es más creíble. Este caso se denomina spear phishing (Rodríguez, 2012)

2.6.2. Scam

En el caso de que el objetivo final, tras conseguir los datos personales, sea económico, un *phisher* cauto no ingresará directamente el dinero en su cuenta, por ello utilizará esta técnica

Este tipo de fraude consiste en que empresas ficticias realizan la captación de personas mediante diversas vías como chats, foros, notificaciones vía correo electrónico, anuncios en periódicos e incluso difusión en webs; donde ofrecen puestos de trabajo con excelentes ventajas y cuyas condiciones se resumen en disponer de un ordenador y ser titular de una cuenta bancaria. Las personas que aceptan este tipo de empleos reciben el nombre de “muleros” y desconocen el carácter ilícito de sus acciones que consiste en el blanqueo de dinero obtenido a través del *phishing* (Rodríguez, 2012).

2.6.3. Spoofing

A diferencia del *phishing*, el *spoofing* también se trata de una suplantación de identidad, pero en la cual no se requiere por lo general de un engaño previo a la víctima o a la entidad. Adicionalmente, los motivos del mismo pueden ser muy variados, desde la estafa a la investigación (Rodríguez, 2012).

Como se ha dicho, normalmente no usa el engaño, por lo que la actuación de forma general es básicamente técnica, menos picaresca y fraudulenta. Por ello suele requerir siempre de unos conocimientos muy avanzados (Rodríguez, 2012)

2.7. LAS REDES SOCIALES

Las redes sociales son una fuente de sustracción de información importante y gracias a ellas y aplicando la llamada ingeniería social, se pueden obtener muchos datos personales que después se utilizarán de forma fraudulenta.

Esta nueva forma de relacionarse con otras personas tiene, por tanto, muchos riesgos. De la misma forma que en la vida real somos precavidos cuando conocemos nuevos amigos, hemos de actuar de igual modo en las relaciones vía web.

El principal inconveniente de este nuevo medio de relacionarse es la falta de privacidad. Es importante hacer una diferencia entre los términos privacidad y seguridad (OSI, 2022).

- “La **privacidad** en la red consiste en la habilidad de cada individuo de controlar que información revela uno mismo en el conjunto de Internet, y controlar quien puede acceder a ella”.

- “La **seguridad** se centra en la confianza de que esas decisiones son respetadas, mediante, por ejemplo, la correcta protección de los datos personales almacenados”.

Como usuarios hemos de adoptar una serie de medidas para evitar que nuestra información personal sea utilizada por “ciber delincuentes” de forma fraudulenta. Para ello, antes de utilizar cualquier servicio de una red social, leeremos sus políticas de privacidad y condiciones de uso. Hemos de ser nosotros los que determinemos nuestro perfil y los límites de nuestra privacidad, grupo de personas que acceden a nuestro perfil, etcétera para protegernos de posibles robos de

identidad; en especial los adolescentes que no son conscientes del alcance que puede llegar a tener la publicación de documentos, fotos e información personal en la web (OSI, 2022).

La publicación de los contenidos es responsabilidad de la persona que los publica, por ejemplo, no se puede publicar fotos de otras personas sin su consentimiento, debido a lo desarrollado es muyes muy importante incorporar dentro de nuestro marco legislativo, la regulación de estos delitos que son consecuencias de las nuevas tecnologías y por ello debemos tener en cuenta que el Derecho debe ser dinámico y estar a la par de la trascendencia de los años (OSI, 2022)

2.8. DEFINICIÓN DE DERECHO PENAL.

Derecho Penal es: "El conjunto de normas jurídicas de derecho público interno, que define los delitos y señala las penas y medidas de seguridad para lograr la permanencia del orden social" (Cabanellas De Torres, 2000).

El criminalista español Eugenio Cuello Calón (2004) lo define como el conjunto de normas que determinan los delitos, las penas que el Estado impone a los delincuentes y a las medidas de seguridad que el mismo establece para la prevención de la criminalidad.

Algunos de los autores distinguen al Derecho Penal, al definirlo entre derecho Penal Subjetivo y Derecho Penal Objetivo. El Derecho Penal en sentido objetivo, es el conjunto de normas jurídicas establecidas por el Estado que determinan los delitos, las penas y las medidas de seguridad con que aquellos son sancionados (Cuello, 2004).

2.9. TEORÍA DEL DELITO CON RELACIÓN A LA SUPLANTACIÓN DE IDENTIDAD

La teoría del delito es un sistema de categorización por niveles, conformado por el estudio de los presupuestos jurídico penales de carácter general que deben concurrir para establecer la existencia de un delito, es decir, permite resolver cuando un hecho es calificable de delito. Esta teoría, creación de la doctrina (pero basada en ciertos preceptos legales), no se ocupa de los elementos o requisitos específicos de un delito en particular (homicidio, robo, violación, etc), sino de los elementos o condiciones básicas y comunes a todos los delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella (Levene & Chiavalloti, 2019).

En ese entendido, el presente capítulo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal, que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de infracciones o delitos, alcance en Bolivia los niveles de peligrosidad que se han dado en otros países.

Al iniciar nuestro trabajo, encontramos que no existe un consenso en cuanto al concepto de delito informático, y que estudiosos del tema lo han definido desde diferentes puntos de vista como son el criminógeno, formal, típico y atípico, etc.; dando lugar a que la denominación de que esta conducta haya sufrido diferentes interpretaciones, las que hemos recogido en la primera parte de la investigación. Además, hemos señalado los sujetos, activos, pasivos, clasificación y los tipos de delitos informáticos considerados tanto en la doctrina como en la legislación de diferentes países (Sarzana, 2019).

2.10. LA USURPACIÓN DE IDENTIDAD COMO TIPO PENAL

El delito de usurpación de identidad en Bolivia, no ha tenido el reconocimiento que merece, de la norma podemos establecer que para que exista suplantación

de identidad basta que haya utilización por parte de un sujeto del nombre de otra persona sin consentimiento de ésta última, independiente de la comisión de otras conductas que también se consideren delictivas y sean consecuencia de este ilícito primigenio.

El término “el que usurpare el nombre de otro” no puede tomarse de manera literal, puesto que debe entenderse más ampliamente abarcando cualquiera de los elementos que conforman la identidad de la persona, ya sea sólo el nombre, la imagen, la firma, etc., o bien una suma de todos o algunos de ellos. Tratándose entonces de una personificación, la que se lleva a cabo no sólo con el uso del nombre ajeno, sino que, teniendo la intención de actuar en nombre de otro, apropiándose de tal identidad como si fuese la suya. También cabe destacar que de la simple lectura del artículo se deduce que la usurpación de identidad se configura con la mera acción de suplantación, independiente del daño que se provoque con ésta a la víctima, ya que el delito se sanciona sin perjuicio de las consecuencias en la fama o intereses que se le ocasionare a la persona cuyo nombre se ha usurpado (Pessó, 2015).

De esta idea se puede establecer que la usurpación de identidad puede conformarse por dos fases, una primera donde existe una utilización de la identidad de otro y que siempre está presente, puesto que el ilícito se configura con la acción de suplantación, y una segunda etapa que está relacionada con el daño que es consecuencia de otros delitos conexos que se hacen valer de la usurpación de identidad para su comisión. Dicho en otras palabras, basta la fase primitiva de suplantación para que se dé el delito, habiendo o no daño para la víctima (el cual puede ser de diversa índole), mientras que la segunda fase es independiente y eventual respecto de la primera, puesto que existirá cuando el ilícito primigenio se utilice para la ejecución de otros delitos (como los de injuria, calumnia, estafa, entre otros), los que generen otro tipo de daño o uno más intenso (Pessó, 2015).

En relación a este punto, y de acuerdo a lo planteado por el precepto, se entiende que de cometerse una usurpación de identidad y otros delitos que atenten contra la fama o intereses de la víctima y que estén conectados con el primero, habrá un concurso ideal de ilícitos, puesto que el sujeto activo se habrá servido de la suplantación para la comisión de los segundos.

2.10.1. Elementos para su configuración

Para un estudio acabado del injusto de usurpación de identidad cabe revisar los elementos que sirven a su configuración:

Sujeto pasivo: La suplantación de identidad en su faceta clásica puede sólo afectar a las personas naturales, puesto que son estas las que detentan una identidad propia y determinada, susceptible de apoderamiento por terceros en cualquiera de los elementos que la representan y conforman (Novoa, 2000).

Sujeto activo: Hacerse pasar por otro es una práctica que sólo pueden llevar a cabo las personas naturales, puesto que únicamente aquellas capaces de intervenir en la comisión del ilícito y ser responsables ante la ley penal. Además, es menester mencionar que no es requisito tener una calidad especial para ser sujeto activo, como detentar el cargo de funcionario público (Novoa, 2000).

Acción u omisión: La figura penal de suplantación de identidad implantará que se sancionara aquel que usurpare el nombre de otro, sólo siendo procedente la acción (por tanto, excluyéndose la usurpación por omisión) de apropiarse de cualquiera de los elementos de configuran la identidad de una persona (Novoa, 2000).

En cuanto a la calidad de este delito, debemos preguntarnos si constituye un ilícito de carácter instantáneo o permanente. Por un lado, si la suplantación se consuma “en un solo instante, esto es, si el proceso de ejecución que culmina al completarse todas las exigencias del tipo delictivo se cierra en un momento determinado y único, nos encontramos en presencia de un delito instantáneo”

(Novoa, 2000). Como en el caso en que un individuo entregue una cédula de identidad de otra persona a la policía cuando esta ejecuta un control de identidad. Por otro lado, estimamos que también es posible que exista una suplantación de nombre de carácter permanente, cuando “el momento consumativo perdura en el tiempo” como en todos aquellos casos en que una persona adopta la personalidad de otro y realiza diferentes actos en su nombre sin la autorización por parte de este último.

Es importante señalar que gracias a la usurpación de identidad el sujeto activo puede cometer un amplio abanico de conductas antijurídicas con la información personal de otro ilegalmente obtenida (siendo todos delitos diferentes pero conexos, en virtud de que se hacen valer de la suplantación de identidad para ejecutarse), las que pueden provocar un gran espectro de daños a la víctima.

Culpa o dolo: En cuanto al elemento subjetivo que debe presentarse en el ilícito en cuestión, “la acción típica, “usurpar” supone necesariamente el uso de la identidad usurpada lo que sólo puede realizarse haciéndose pasar por otro”, con la intención de hacer uso de los derechos y acciones del suplantado (Novoa, 2000).

Daño: El precepto penal examinado estipula que la suplantación de identidad se configurará por el sólo hecho de “usurpar”, lo que se traduce en el que la acción delictiva se sancionará independiente de que sufra daño o no el sujeto pasivo. Incluso, el afectado podrá demandar separadamente por el perjuicio que se le produzca en su fama o intereses cuando éste sea consecuencia de otros delitos cometidos por el delincuente aprovechándose de la usurpación de identidad ya ejecutada (Novoa, 2000).

Se puede encontrar que en la relación que existe entre el delito de usurpación de identidad y el daño producido por éste, existen dos escenarios diametralmente opuestos. En un primer caso, puede ocurrir que la suplantación sea penada aun cuando no produzca ningún daño o cuando éste sea mínimo, mientras que en un

segundo caso, la ejecución de la usurpación puede conllevar un perjuicio inmensurable a la víctima, ya sea porque la mera suplantación le afecta en su ámbito más personal, o bien, porque en virtud de delitos conexos a la misma se le provoca un daño en su honor o su patrimonio que exceden la magnitud del daño que se produciría sólo con el delito originario

El bien jurídico protegido.-el tipo penal en cuestión es el derecho a la identidad personal, que tiene por fundamento la "verdad de la persona" (Cabanellas De Torres, 2000)

Asimismo, en palabras de Garrido Montt la norma protege "la vida en relación, pues en el tráfico jurídico la ocultación de la propia identidad mediante el empleo de un nombre que no corresponde al real, puede provocar serias confusiones en la sociedad" (Garrido, 2005)

Por consiguiente, lo que se persigue resguardar, es la autenticidad de los sujetos y el aspecto de la personalidad que se proyecta en la vida en sociedad, el que se manifiesta en los diferentes elementos identificativos de la misma (como por ejemplo el nombre o la imagen) los que nos individualizan como seres únicos e irrepetibles.

2.11. ASPECTOS JURÍDICOS Y SOCIALES

Cuando una persona se hace pasar por otra con el fin de obtener un beneficio propio, se está cometiendo un delito de suplantación de identidad. Esta acción puede tener la intención de cometer otros hechos que ya constituyen delitos en sí mismos, pero también para la contratación de servicios de telefonía, para obtener una hipoteca o un crédito, para efectuar compras tanto en tiendas físicas como a través de tiendas online, etc.

En internet, y gracias a las facilidades para crear perfiles en redes sociales con apenas una dirección de correo electrónico (cualquier dirección de correo electrónico), la suplantación de identidad se ha multiplicado. Es bastante habitual

que alguien utilice fotografías de otra persona sin su consentimiento expreso y cree un perfil en Twitter, Facebook o cualquier otra red, incluso utilizando también su nombre, y haga uso de esta cuenta para insultar, acosar a terceras personas y hasta para lograr hacerse con datos personales y bancarios de otros usuarios con los cuales continuar cometiendo sus fechorías (Calderon, 2021).

Las penas contempladas para este delito son muy variadas en función de las circunstancias de los hechos. Por ejemplo, el uso de una fotografía de otra persona sin su consentimiento supone un delito de vulneración del derecho a la propia imagen (regocijo por el artículo 18 de la Constitución española) y contempla penas de hasta tres años de cárcel. Lo cual en nuestra jurisprudencia se carecen completamente.

Sin lugar a dudas, estos cambios sociales profundos se tienen que reflejar a través de modificaciones serias en el ordenamiento jurídico, como sucede por ejemplo, con el surgimiento de la legislación medioambiental o las normas que rigen a las tecnologías de la información. Ante ello, la rama del Derecho no puede negarse a la capacidad de interpretar mejor las necesidades humanas y de adaptarse en forma más perfecta a lo que de él se requiere para el bien común, la paz, la justicia y el progreso (Núñez Ponce, 2007).

La revolución tecnológica ha redimensionado las relaciones entre los hombres. Se está ante una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de la cultura, hasta el punto de que para designar el marco de la convivencia se alude reiteradamente a la expresión *Sociedad de la Información* (Herrera, 2004)

2.12. DESARROLLO DEL DELITO CIBERNÉTICO

Como indica Alvin Toffler, el proceso de cambio en todos los órdenes de la sociedad se ha acelerado enormemente, esto es, ocurren cada vez más cambios en menos tiempo. Uno de los motores de este cambio es la tecnología,

alimentada, a su vez, por el conocimiento, que también crece en forma exponencial (Toffer, 2000).

Según estimaciones de expertos en seguridad cibernética de las Naciones Unidas, aproximadamente el 80% de todos los delitos cibernéticos está siendo cometido por pandillas sofisticadas de criminales que participan en operaciones altamente organizadas. Las pandillas operaban igual que las empresas legítimas, ya que mantenían horas laborales regulares con una jerarquía de miembros, trabajando en conjunto para crear, operar y mantener cualquier fraude en el que se centraban (OSI, 2022).

El crimen se esconde justo debajo de la superficie de internet. Es como un hongo que no puedes ver, extendiéndose a través de la web una brecha a la vez. La razón por la que es capaz de propagarse de la manera en que lo hace se reduce a una serie de factores. En primer lugar, los criminales pueden esconderse fácilmente detrás de sus terminales lejos de los reguladores, operando con impunidad, utilizando software de última generación y técnicas de redes para enmascarar sus ubicaciones, y desviar cualquier mirada indiscreta. En segundo lugar, internet proporciona el acceso fácil a casi todos en el planeta y, cuando vamos al meollo del asunto, cualquier persona con el dinero o la información para robar está probablemente conectada y no es difícil de encontrarla. En tercer lugar, si deseas ejecutar una estafa, no tienes que ser un programador, todo lo que tienes que hacer es saber dónde comprar uno.

Internet es multicapa, está la capa superficial a la que cualquiera puede llegar, pero luego hay capas más profundas que son mucho más difíciles de encontrar, están la Web Profunda y la Web Oscura, donde las actividades ilegales se producen a diario. No estoy hablando de un área de acceso solo para miembros, es fácil encontrarlo, estoy hablando de sitios web que no se preocupan por su SEO, no les importa si el mundo entero puede encontrarlos e incluso tratan de ocultar activamente sus sitios del público dentro de la red TOR u otras capas de internet. Estos sitios incluyen todo lo imaginable, desde salas de chat inocentes

donde los miembros quieren permanecer completamente anónimos, a sitios donde puedes comprar tu propio malware (OSI, 2022).

2.13. CONCEPTOS BÁSICOS DE DERECHO

Para un adecuado proceso de investigación, respecto a la edad de punibilidad, y otros aspectos que configuran el ilícito planteado de suplantación de identidad, es imprescindible conceptualizar los siguientes términos (Ossorio, 1990):

Identidad: Circunstancia de ser una persona o cosa en concreto y no otra, determinada por un conjunto de rasgos o características que la diferencian de otras.

Persona: Es aquel ser o ente a quien el ordenamiento jurídico le reconoce voluntad para ser titular de derechos subjetivos y de deberes. (Escuela alemana)

Suplantación de Identidad: Es una expresión informática que se emplea para referirnos a los abusos informáticos cometidos por delincuentes para estafar, obtener información personal, contraseñas, de forma ilegal.

Delito: La palabra "delito", deriva de *delictum* del verbo *delinquere*, a su vez compuesto de linquere, dejar y el prefijo de, en la connotación peyorativa, se toma como linquere viam o rectam viam: dejar o abandonar el buen camino"

El delito para Jakobs es no más que el quebrantamiento de la vigencia de la norma. Se presenta como una perturbación social provocada por el apartamiento del rol por parte de su portador. El delito supone una comunicación defectuosa, una expresión de sentido entre personas, desnaturalizada por la norma. El delito no supone un suceso entre seres humanos, como así también no está determinado por la afectación a un bien jurídicamente protegido. El delito es la desautorización de la norma o falta de fidelidad al ordenamiento jurídico actuado (Jakobs, 1997)

Según Alimena: "Una vez escrita la ley, es delito todo hecho prohibido bajo la amenaza de una pena" (Alimena, 1915).

Según Beling: "Delito es una acción típica, antijurídica, culpable, cubierta con una sanción penal adecuada a la culpabilidad, y que llena las condiciones legales de punibilidad" (Beling, 2002)

Según Bentham: "Un acto prohibido (por los legisladores) es lo que se llama delito".

Culpabilidad: El concepto de la culpabilidad, dependerá de la teoría que se adopte, pues no será igual el de un psicologista, el de un normativista o el de un finalista. Así, el primero diría, la culpabilidad consiste en el nexo psicológico que une al sujeto con la conducta o el resultado material, y el segundo, en el nexo psicológico entre el sujeto y la conducta o el resultado material, reprochable, y el tercero, afirmaría, que la culpabilidad es la reprochabilidad de la conducta, sin considerar el dolo como elemento de la culpabilidad, sino de la conducta. La culpabilidad en la tesis finalista se reduce a la reprochabilidad y a diferencia de la teoría normativa el dolo y la culpa no son elementos de la culpabilidad porque son contenido del tipo. "la culpabilidad es, por lo tanto, responsabilidad, apartándose consecuentemente de los normativistas mantienen el dolo y la culpa en la culpabilidad, constituyendo como se afirma por un sector un *mixtum compositum,* de cosas no pueden mezclarse". El concepto de culpabilidad como tercer aspecto del delito y de acuerdo a la definición anterior, nos señala cuatro importantes elementos que la conforman y son: una ley, una acción, un contraste entre esta acción y esta ley, y el conocimiento de esta situación (Betancourt López, 1994).

La culpabilidad es un elemento básico del delito y es el nexo intelectual y emocional que una al sujeto con el acto delictivo (González de la Vega, 1996).

Imputabilidad: *Von Liszt*, Define diciendo" que es la capacidad de conducirse socialmente; observando una conducta que responda a las exigencias de la vida común. (Listz, 1999)

Según Jiménez de Asúa, afirma que: “Imputar un hecho a un individuo es atribuírselo, para hacerle sufrir las consecuencias; es decir, para hacerle responsable de él, puesto que de tal hecho es culpable. La culpabilidad y la responsabilidad son consecuencias tan directas, tan inmediatas de la imputabilidad, que las tres ideas son a menudo consideradas como equivalentes y las tres palabras como sinónimas” (Jimenez De Asua, 2018)

Según Zaffaroni, dice de la imputabilidad que: Entendida como capacidad de culpabilidad- tenga dos niveles, uno que debe ser considerado como la capacidad de comprender la antijuridicidad, y otro que consiste en la capacidad para adecuar la conducta a la comprensión de la misma. Cuando Falte la primera capacidad nos faltará la culpabilidad por ausencia de la posibilidad exigible de comprensión de la antijuridicidad; cuando falte la segunda capacidad, nos hallaremos con un supuesto de estrechamiento del ámbito de autodeterminación del sujeto, en este caso, por una circunstancia que proviene de su propia incapacidad psíquica (Zaffaronni, 1999)

2.14. DELITOS INFORMÁTICOS

En el ámbito internacional se considera que no existe una definición propia del delito informático, pero, al consultar bibliografía, en específico del español Carlos Sarzana, en su obra Criminalitá e tecnología, los crímenes por computadora comprenden “cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo” (Sarzana, 2019).

Nidia Callegari define al “delito Informático” como “aquel que se da con la ayuda de la informática o de técnicas anexas” (Callegari, 1985).

Rafael Fernández Calvo define al “delito informático” como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando el elemento informático o telemático contra los

derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española" (Collado, 2018)

María de la Luz Lima dice que el "delito electrónico", "en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin" (Collado, 2018)

Julio Téllez Valdés conceptualiza al "delito Informático" en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tiene a las computadoras como instrumento o fin" (Collado, 2018)

2.15.1. Doctrina jurídica

La doctrina estudia los manantiales de donde brota el derecho: investiga el papel histórico y las relaciones existentes entre las diversas fuentes; esclarece el significado de las normas y elabora, para entender en toda su extensión, el significado de los modelos jurídicos (Felipe, 2020).

Entonces se puede decir que los Fundamentos Jurídico-Doctrinales, son los principios y bases que esclarecen el significado de la norma, pues estudia el origen de donde brota el derecho.

2.15.2. Política Criminal:

Se refiere al conjunto de medidas de hecho y derecho de las que se vale el estado para enfrentar la criminalidad, para controlar, reprimir y prevenir el delito. Para luchar contra el delito es necesario conocer sus causas para así evitar las consecuencias por ende una política criminal que prescinda de la criminología no

es concebible. La política criminal busca y pone en práctica los medios y las formas más adecuadas para hacer eficaces los fines del Derecho Penal (Luna, 2021).

2.16. SANCIÓN PENAL:

La sanción penal es todo aquel castigo o pena, que se establecen en la ley, y que imponen los jueces penales, a los responsables de haber cometido un delito. La sanción penal se impone mediante una sentencia, una vez concluido el proceso penal y cuando el acusado resulto culpable de haber cometido determinado delito. Sanciones penales: Pena de prisión, multa, reparar el daño cometido, trabajar en favor de la comunidad determinado número de horas, prohibición de ir a determinado lugar y algunas más (Ossorio, 1990)

CAPITULO III

MARCO JURÍDICO

MARCO JURÍDICO

El universo de las comunicaciones ha adquirido en nuestra época una magnitud tal, que, para ser comprendido desde el punto de vista jurídico, ya no puede valerse la didáctica del derecho, como en épocas pasadas, sólo del derecho individual de publicar las ideas por la prensa sin censura alguna.

La revolución tecnológica a la que asistimos y en la que estamos inmersos en el presente, merced a los continuos progresos en el campo de las ciencias informáticas, ha hecho posible, entre otras cosas, la creación, acceso y entrecruzamiento de todo tipo de informaciones es el sustrato cultural del cual surge la necesidad de contar con una nueva rama del derecho que regule este nuevo campo de actuación de las normas jurídicas.

3.1. DECLARACIÓN UNIVERSAL DE DERECHO HUMANOS

Declaración Universal de Derechos Humanos Adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948 (ONU, 2009)

Considerando que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana .

Artículo 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (ONU, 2009)

Este Artículo señala que las personas tienen derecho a la protección de la Ley y sus datos personales.

3.2. LA ORGANIZACIÓN DE LAS NACIONES UNIDAS.

Esta organización internacional ha considerado los siguientes delitos, alertando a sus países miembros que se vele por ellos a través de la legislación específica (UNODC, 2004):

A. Fraudes cometidos mediante manipulación de computadoras:

1. Manipulación de datos de entrada

2. Manipulación de programas

3. Manipulación de datos de salida

4. Fraude por manipulación informática

B. Fraudes informáticos

1. Como objeto

2. Como instrumento

C. Daños y modificaciones de programas o datos computarizados.

3.3. EL CONVENIO SOBRE LA CIBER-CRIMINALIDAD

Firmado en Budapest, Hungría, el 23 de noviembre de 2001, por los países integrantes de la Unión Europea y Estados participantes, en la que emite sus recomendaciones sobre el trato que deberá llevarse frente a los Delitos Informáticos, en el cual sus principales objetivos son (OEA, 2001):

- Reafirmar la estrecha unión entre las naciones de la Unión Europea y países firmantes para enfrentar la Cibercriminalidad.
- Intensificar la cooperación con los estados miembros.

- Prioridad en unificar una política penal para prevenir la criminalidad en el ciberespacio con una legislación apropiada y mejorar la cooperación internacional.
- Concientizar a los Estados miembros de los cambios suscitados por la convergencia y globalización de las redes.
- Concientizar sobre la preocupación del riesgo de las redes informáticas y la informática electrónica de ser utilizadas para cometer infracciones penales, ser almacenados y exhibidos.
- Fomentar la cooperación entre los Estados e industrias privadas en la lucha contra la cibercriminalidad y la necesidad de protección del uso de la Informática para fines legítimos al desarrollo de la tecnología.
- Concientizar que la lucha contra la Criminalidad requiere la cooperación internacional en materia penal asertiva, rápida y eficaz.
- Persuadir sobre la necesidad de un equilibrio entre los intereses de la acción represiva y el respeto de los Derechos del Hombre garantizado en el convenio para la protección de estos derechos y libertades fundamentales y reafirmar el derecho de no ser perseguido por la opinión pública, la libertad de expresión, libertad de búsqueda y el respeto a la vida privada.
- Complementar los convenios anteriores, relacionados con la materia o que otorguen soporte, con el fin de hacer más efectiva la investigación, procedimientos penales y recolección de pruebas electrónicas.
- Persuadir sobre la necesidad de mantener y proteger la confiabilidad, integridad y disponibilidad de los sistemas de cómputo, bases de datos, computadoras y redes.

3.4. MARCO JURÍDICO BOLIVIANO

3.4.1. Constitución Política del Estado

En Bolivia no existe una ley específica acerca de la privacidad de datos así mismo con las personas, pueden estar protegidas contra los delitos que involucren datos personales limitándose solo a CPE Art. 21 Inc. 2. “Las Bolivianas y los bolivianos tienen los siguientes derechos: A la privacidad, intimidad, honra, honor, propia imagen y dignidad.” (Gaceta Oficial de Bolivia, 2009)

Sección III: Acción de protección de privacidad

Artículo 133

I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal y familiar, a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

Artículo 134

I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevará en revisión de oficio ante el Tribunal Constitucional Plurinacional, en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo a lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme a lo dispuesto por este artículo, quedará sujeta a las sanciones previstas por la ley.

Se puede observar que los delitos informáticos son abordados desde un punto de vista secundario y casi no son nominados de esta forma directa.

3.4.2. Ley de Telecomunicaciones

En esta ley en el Título IV capítulo II, hace referencia al gobierno electrónico y software libre, Artículo 77 (software libre), en donde todavía no se hace el tratamiento de los delitos informáticos. En el capítulo tercero el de los documentos y firmas digitales, tampoco se toma en cuenta los delitos informáticos; es más en el capítulo cuarto se hace referencia al comercio electrónico en donde en el Artículo 88 (Controversias) se dice que si existiesen se debería acudir a la jurisdicción ordinaria; esto quiere decir a la ley 14379 que es el código de comercio boliviano y si se daña algún bien jurídico protegido se recurrirá al código penal boliviano y se lo tipificará de acuerdo al delito que se haya cometido.

Por lo tanto, una ley dedicada a lo que son los delitos informáticos no se tiene en Bolivia, solo se tienen leyes diferidas de acuerdo a cada uno de los casos en los que se vayan a tipificar.

Realizando todo este análisis se puede observar que no existe en nuestra legislación la figura legal de la evidencia digital y menos existe una sanción a este tipo de acciones antijurídicas.

3.4.3. Código penal boliviano.

En Bolivia, para hacer frente a la delincuencia relacionada con la informática, se adoptó la estipulación de dos artículos insertos dentro de nuestro código penal boliviano vigente :

- **Artículo 363 Bis. (Manipulación Informática).** El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días.

- **Artículo 363 Ter. (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).** El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos (200)días.

Por lo que se realiza un análisis de dicho Artículo, ya que en la reforma del código penal se ha introducido esta figura por el desarrollo de la informática que ha ido evolucionando de forma progresiva. La tecnología con el empleo de procedimientos precisos y rápidos que usados legalmente alivian el trabajo y dan mayor seguridad en la obtención de datos, también la misma usada ilícitamente da lugar a la comisión de delitos a veces de gran volumen.

Este delito es de resultado por su naturaleza y por decisión de la ley porque si no hay resultado no hay una transferencia patrimonial ilícita, no hay consumación pero puede darse la tentativa, es decir realizar la manipulación pero

no alcanzar el fin propuesto. En cierto modo se parece el enriquecimiento ilícito o sin causa justa.

Es delito que excluye toda posibilidad de culpa. La antijurídica radica en que intencionalmente se manipula datos informáticos para lograr resultados incorrectos o evitar un procesamiento correcto a fin de lograr de modo ilícito una transferencia patrimonial en perjuicio de tercero que sufre un detrimento patrimonial, es por esta razón que se ha incluido entre los delitos contra la propiedad.

La manipulación de datos en manejarlos alternado el procesamiento o haciéndolos errar desviando el resultado verdadero, lo que evidentemente en muchos casos como en cuentas bancarias determinan transferencias incorrectas mermando el patrimonio de terceros o de los mismos bancos.

Por lo que:

- **Sujeto activo:** Cualquier persona (presidentes de bancos, ingenieros en sistemas, ingenieros electrónicos, programadores, operadores de terminales y otros).
- **Sujeto pasivo:** Persona afectada o sector afectado (mundo de los negocios).
- **Delito:** Impropio
- **Elemento Subjetivo:** Dolo
- **C.S.Q.:** Manipule datos informáticos para lograr resultados incorrectos o evitar un proceso correcto a fin de lograr ilícitamente una transferencia patrimonial.
- En perjuicio de un tercero.
- **Verbo nuclear**: Obtener, manipular.
- **Bien jurídico protegido**: La propiedad.
- **Sanción:** Reclusión de 1 a 5 años y multa de 60 a 200 días.

Artículo 363 ter.- (alteración, acceso y uso indebido de los datos informáticos).

El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

3.5. LEGISLACIÓN COMPARADA.

La problemática de los Delitos informáticos en la actualidad posee un alcance global o mundial y su desarrollo exponencial hace necesaria que otros países cuenten con la legislación apropiada. Entre ellos se destacan, Chile y España. En nuestra búsqueda de nuestra legislación pertinente y adecuada a nuestra.

3.5.1. Chile

En Chile el manejo inadecuado de la información ha sido penalizado a través de la Ley 19.233 Contra delitos Informáticos vigente desde 17 de junio de 1993. Pionera en América, Latina es objeto de crítica por la ubicación de su texto fuera del código penal, en franca violación del principio de unificación que propugna la codificación. Se estaría dejando un código penal desadaptado a las necesidades de la sociedad y afectando también la labor del juez y la defensa de los inculpados. Compuesta de cuatro artículos, introduce figuras tales como (BCN Chile, 2022):

1) La destrucción o inutilización de los datos contenidos dentro de su computadora

2) El apoderamiento o uso indebido de la información,

3) La alteración, daño, destrucción de los datos de un sistema de tratamiento de información,

4) Y la revelación de datos contenidos en un sistema de información.

3.5.2. España

Este país cuenta con un desarrollo enorme en la materia. La Constitución Española en su Título I, Capítulo segundo Derechos y Libertades, sección primera de los Derechos Fundamentales, y las libertades públicas artículo 18, establece lo siguiente: Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. La ley limitará el uso de informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (CEA, 2018)

De esta manera, otorga la posibilidad de que la ley limite el uso de la informática para proteger el honor e intimidad, tanto personal como familiar, de los ciudadanos.

En el nuevo Código Penal español (aprobado por Ley - Orgánica 10/1995, de 23 de noviembre) se introducen varios artículos relacionados con el tema que estamos tratando (CEA, 2018).

Entre las penalizaciones incluidas, se destacan las siguientes: Delitos contra la intimidad y el secreto de las comunicaciones (art. 197). Estafas electrónicas. Infracción de los derechos de propiedad intelectual. Delito de daños. Revelación de secretos contenidos en documentos o soportes informáticos. Falsedad en documento electrónico. Sustracción, destrucción, inutilización u ocultación de documentos electrónicos por parte de funcionario público cuya custodia le esté encomendada por razón de su cargo (CEA, 2018).

Este artículo también sanciona a las personas que leen mensajes privados de usuarios sin su consentimiento y cuya sanción es de uno a cuatro años de prisión. También se castiga la destrucción de datos realizada con intención; entran también en esta categoría los virus y la ruptura de sistemas. Además, se protege la intimidad personal sancionando la difusión de datos personales sin autorización (1 - 4 años) (CEA, 2018).

CAPITULO IV

MARCO PRÁCTICO

4.1. Trabajo de Campo

4.1.1. Población de estudio

Se denomina población al conjunto de todos los casos que concuerdan con determinadas especificaciones, mismas que pueden ser de contenido, lugar y tiempo en una determina investigación en el caso concreto de la presente investigación el universo de estudio esta dado por todas las personas que pueden tener relación con el recojo y colección de pruebas e indicios, su resguardo y la disposición final de la misma en este

En este universo se consideran a ciudadanos bolivianos mayores de 18 años, residentes de la ciudad de La Paz lo que según datos el INE llegan a un total de 405.287 personas

4.1.2. Muestra de estudio

La muestra de estudio es el subgrupo del universo, del cual se recolectan los datos específicos a la investigación realizada y debe ser representativo del universo del cual ha sido tomada (Hernández y otros, 2014), en el caso de la presente investigación esta dado por una muestra p´robabilistica de universo conocido, la misma que para su determinación recurre a la siguiente formula estadistica de determinacion muestral:

$$\boldsymbol{n = \frac{Z^2 * p * q * N}{e^2(N) + Z^2 * p * q}}$$

Dónde:

n = muestra requerida para el estudio.

Z = Nivel de confianza del 95 %, distribución de Gauss de 1,96.

e = Error de estimación (precisión en los resultados) 5 % = 0,05.

p = Probabilidad de éxito 50% = 0,50.

q = Probabilidad en contra, 50% = 0.5.

N = Población = 405.287

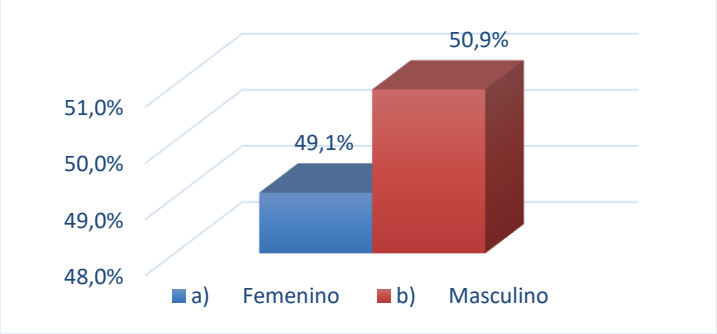
De donde se determina que la muestra la conforman un total de 381 estantes y habitantes del municipio de La Paz, que en este caso tienen más de 18 años, residen en la ciudad de La Paz, cuentan con una cuenta de correo electrónico y/o realizan transmisión de información, comunicación e interacción en medios digitales

4.2. Resultados de las encuestas

Las encuestas realizadas han arrojado los siguientes resultados:

1. **Genero de los encuestados:**

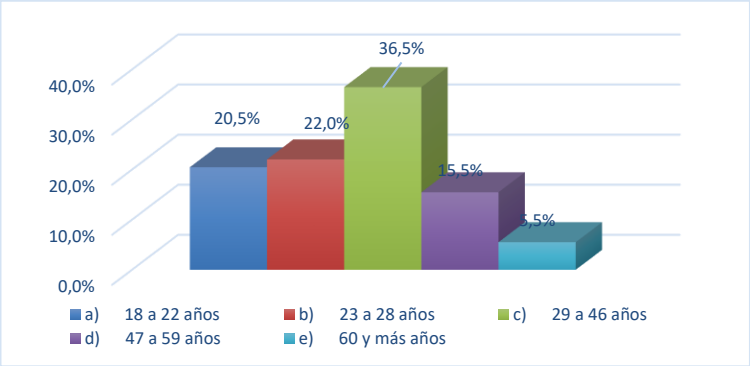
Gráfico 1: Genero de los encuestado



La encuesta se ha realizado en la ciudad de La Paz, según los estudios que analizan la situación del uso de internet en Bolivia, se tiene que hasta el año 2021, Bolivia contaba con 12.16 millones de conexiones a telefonía móvil (celular), 5.58 millones de habitantes acceden a internet, 8.20 millones de habitantes son usuarios activos de redes sociales, es decir el 69.8% de la población total de Bolivia. Ahora de este total de personas que usan redes sociales, el 47.4% son del género femenino y el 52.6% del género masculino; porcentaje similar a la participación en la encuesta realizada en este estudio, donde, el 50, 9 % son participantes varones y el 49,1 % son mujeres

2. Rango de edad de los participantes

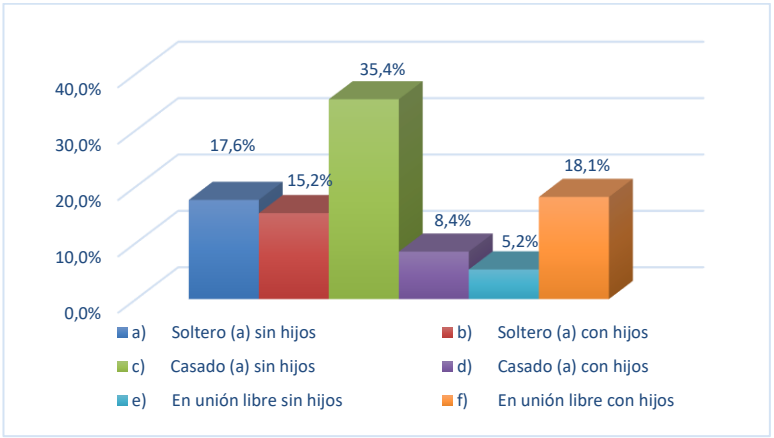
Gráfico 2: Rango de edad de los participantes



De acuerdo a los resultados de la encuesta realizada, los participantes que han sido parte de ella, se encuentran mayoritariamente (35,5%) en un rango de edad de entre los 29 y 46 años, el 22 % son personas que están en el rango de 23 a 28 años, el 20,5 % son personas entre 18 y 22 años de edad. El rango etario de 47 a más años sima un 21 %.

3. Status social de los encuestados

Gráfico 3: Status social de los encuestados

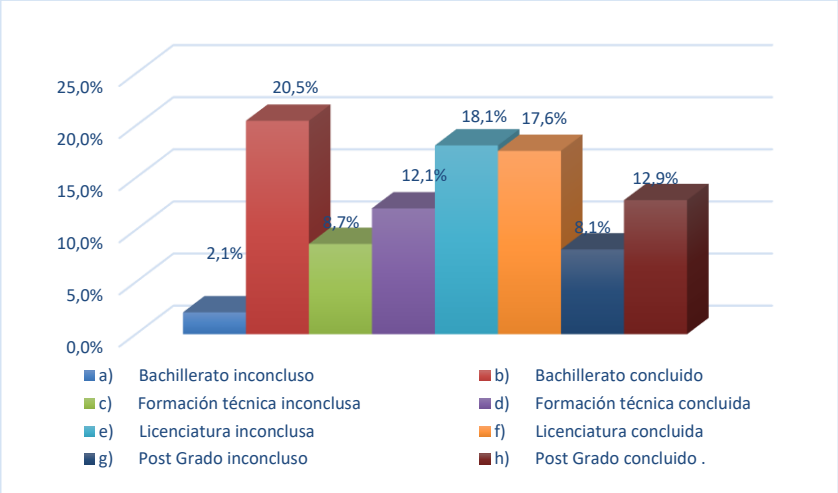


Dentro de los encuestados el 35,4 % de la población son personas casadas que no tienen hijos, el 18,1 % son personas que viven una relación de unión libre pero tienen hijos en común con la pareja que comparten vida, el 17,6 % son

personas solteras que no tienen ningún tipo de descendencia que dependa de ellos, solo el 8,4 % manifiestan ser personas casadas con hijos fruto de la unión matrimonial, finalmente el 5,2 % son personas que viven en unión libre pero no tienen hijos en común entre los miembros de la pareja

4. Grado de instrucción o formación profesional

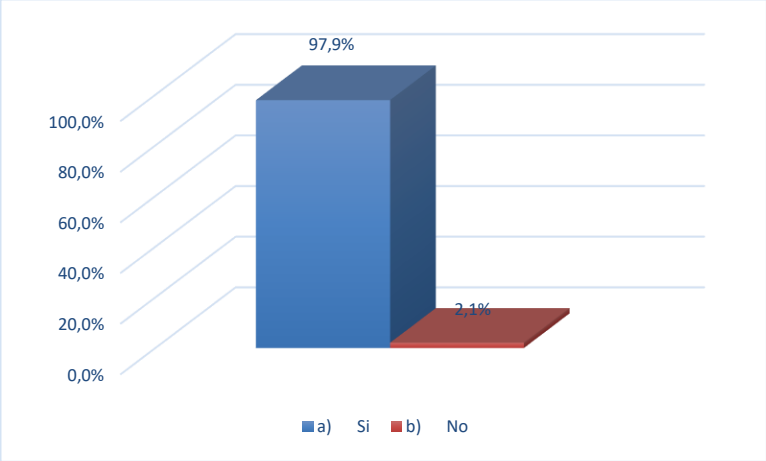
Gráfico 4: Grado de instrucción o formación profesional



En la medida de que la población reciba mayor información respecto de los riesgos del manejo de las redes sociales, será más fácil prevenir delitos tales como la suplantación de identidad, de ahí importante conocer cual es el grado de formación que tiene los participantes, en tal sentido los resultados de las encuestas realizadas determinan que, el 20,5% de los encuestados ha concluido el bachillerato, el 18,1 % está en proceso de estudio para conseguir un nivel académico de licenciatura, el 17,6% ya ha concluido la licenciatura, el 12,1 % tiene formación técnica concluida, el 12, 9 % ha concluido estudios de post grado. Estos resultados muestran que el grupo poblacional encuestado son personas que han recibido una formación educativa acorde a conocer los riesgos del uso de las redes sociales y los medios digitales en los que se transmite información, en muchos casos, personal.

5. Uso de correo electrónico y redes sociales

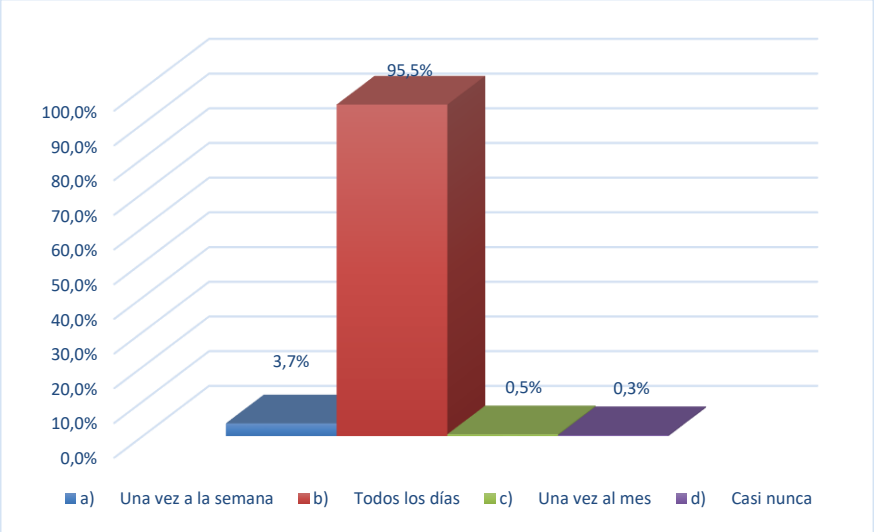
Gráfico 5: Uso de correo electrónico y redes sociales



Las redes sociales más utilizadas en Bolivia son Facebook, Twitter, YouTube, Pinterest e Instagram, según la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) Autoridad de en 2022, 8,45 millones de personas utilizan las redes sociales en Bolivia, lo que representa el 70,9% de la población boliviana, de esta población, el 95.3 % de las personas que utilizan las redes sociales son mayores de 13 años. Esta realidad se corrobora con el trabajo de campo realizado donde el 97,9 % de los encuestados cuenta con correo electrónico o algún tipo de red social; en consecuencia, el gran número de personas que participan en el intercambio dinámico de información y datos por medio de plataformas digitales, hacen que el riesgo de sufrir delitos informáticos sea mayor para la población en general, solo el 2,1% manifiesta no estar conectado a ningún tipo de medio digital, esto debido a malas experiencias sufridas o la falta de tiempo que los obliga a no tener este tipo de conectividad.

6. Frecuencia de uso de medios digitales y redes sociales

Gráfico 6: Frecuencia de uso de medios digitales y redes sociales

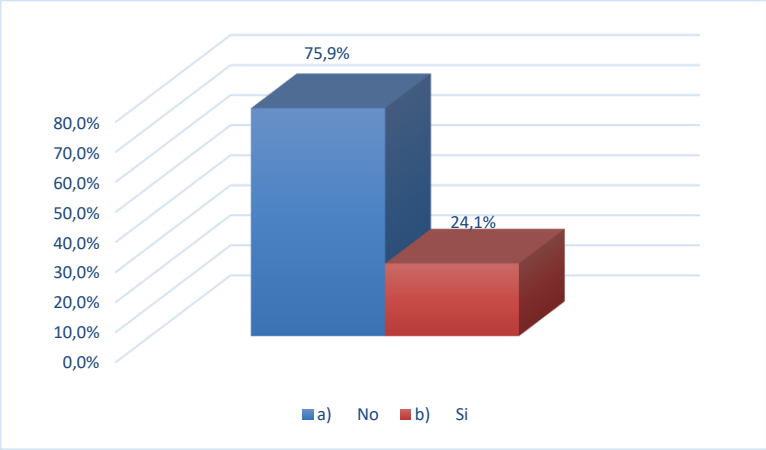


Considerando que las redes sociales y los medios digitales son frecuentemente utilizados para estar en contacto con amigos, para mantenerse al día con noticias ya que han sustituido, en muchos casos, a los noticieros de radio, televisión y prensa escrita, y que actualmente se usan para realizar transacciones financieras o negocios por medio de redes sociales o correos electrónicos, el uso de las tecnologías de información y comunicación es cada vez más frecuente.

Así, se tiene que, según la encuesta realizada el 95,5 % de los participantes refieren que se conectan a redes sociales, correos electrónicos y/o algún otro medio digital todos los días, el 3,7% de los encuestados manifiesta que lo hacen una vez por semana, solo el 0,5% manifiesta que esta conexión la realiza una vez al mes y el 0,3% manifiesta que no se conectan con frecuencia.

7. Precaución usada para proteger el acceso las cuentas de medios digitales

Gráfico 7: Precaución usada para proteger el acceso las cuentas de medios digitales



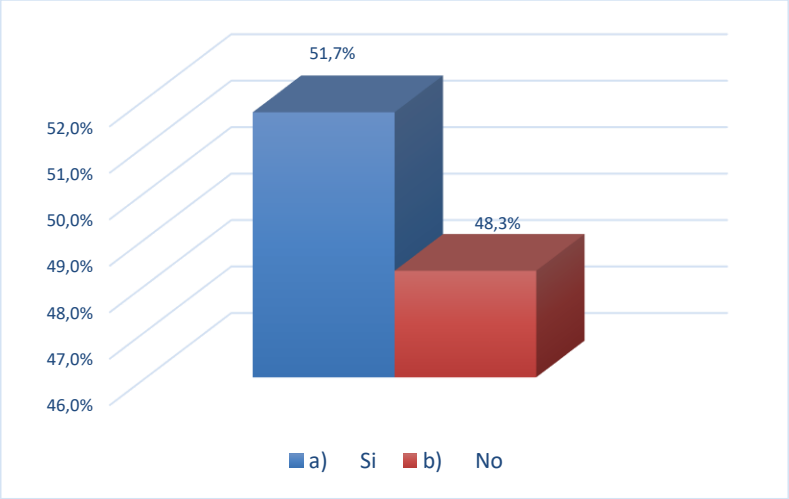
La suplantación de identidad o phishing en redes sociales pretende, por medio de una actividad delictiva obtener beneficios económicos, dañar la reputación o acceder a datos bancarios de las personas; según el Observatorio de Delitos Informáticos de España,, en coordinación con la Organización de Naciones Unidas han determinado que, solo en el año 2020, el número total de delitos informáticos ascendió a casi 288.000 en España y en una cifra similar se ha dado en muchos países del mundo, lo que lleva a solicitar a los usuarios de redes sociales y otras formas de comunicación y transmisión de información vía internet, protejan sus cuentas personales tomando recaudos efectivos para evitar el robo de identidad; así, se recomienda limitar el tipo de información personal que se publica, cambiar las contraseñas con frecuencia, no aceptar solicitudes de personas desconocidas y revisar los permisos y la configuración de privacidad de las cuentas.

En la encuesta realizada en el presente estudio, el 75,9% de los encuestados manifiesta que no toman recaudos de seguridad para proteger su identidad y sus contraseñas en los medios digitales y redes sociales donde comparten información, lo que los hace vulnerables a cualquier tipo de delito informático; solo

el 24,1, % del los encuestados manifiesta que cuidan la información que publican y tratan de resguardar sus contraseñas para evitar algún tipo de conflicto posterior.

8. **Ha sido victima de accesos indeseados a sus cuentas de redes sociales o medios digitales**

Gráfico 8: Ha sido víctima de accesos indeseados a sus cuentas de redes sociales

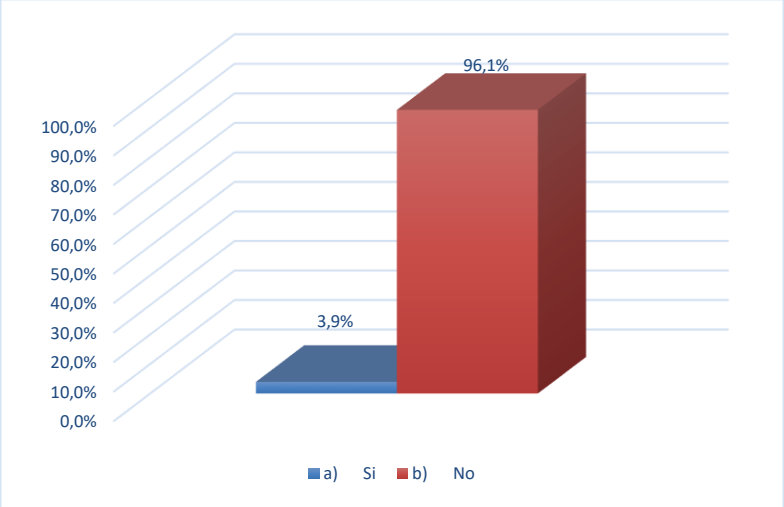


De acuerdo a las encuestas realizadas el 51,7 % de los participantes manifiesta que alguna vez han sufrido el acceso indebido o indeseado de una tercera persona a sus cuentas personales en redes sociales, correos electrónicos u otros medios digitales, la mayoría de los afectados, refiere que no han tenido consecuencias graves, algunos manifiestan que han tenido complicaciones para recuperar sus información y algunos manifiestan que han perdido en definitiva el acceso a sus cuentas o han tratado de estafarlos por medio de mensajes que les han llegado utilizando información recopilada de sus redes sociales.

El 48,3% manifiesta que hasta ahora nunca han tenido dificultades con el manejo de sus redes sociales o contraseñas de medios digitales, cuando mucho refieren haber olvidado sus contraseñas lo que los ha llevado a tener que abrir nuevas cuentas de redes sociales, pero eso es más un error personal que un delito cometido por terceros, aunque es también un factor de inseguridad.

9. Denuncia de acceso indebido a cuentas digitales personales

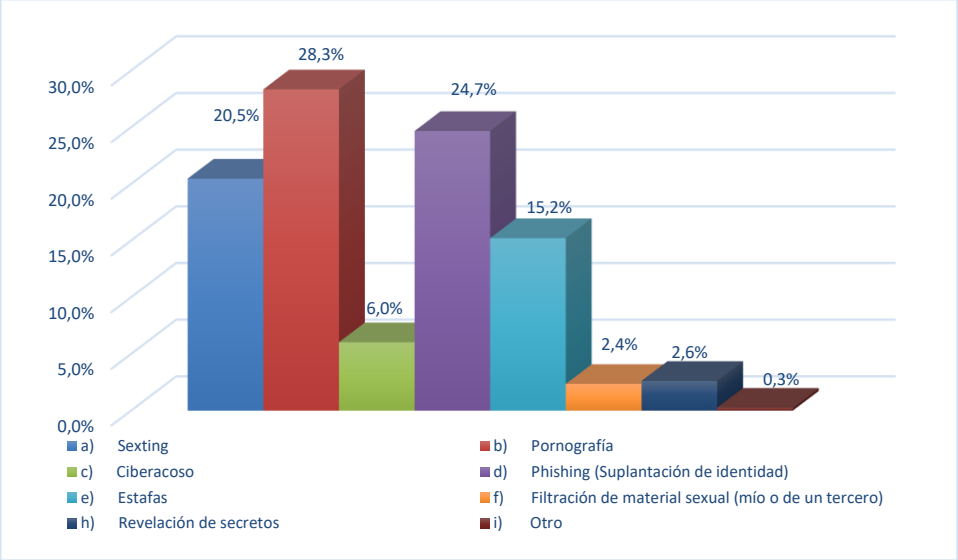
Gráfico 9: Denuncia de acceso indebido a cuentas digitales personales



Existen varias razones por las que no se denuncian los delitos informáticos, una de ellas es la dificultad para identificar al autor o a la víctima de estos delitos, ya que muchas veces se usan medios anónimos o los usuarios de internet son lo suficientemente hábiles como para esconder su procedencia. Otra razón es el desconocimiento de la legislación aplicable o de los procedimientos para presentar una denuncia en Bolivia, también influye el temor a perder el prestigio, la reputación personal. Ahora, de acuerdo a los resultados obtenidos en la encuesta realizada, el 96,1 % de los encuestados manifiesta que no ha denunciado o no denunciaría un caso de cibercrimen o algún tipo de acceso indebido a sus cuentas personales, esto se fundamenta en que: primero no conocen como hacer su denuncia, no saben cual es el procedimiento ni los requisitos necesarios para realizar esta acusación, no conocen si hay o no una ley que sanciones este tipo de delitos o porque simplemente no creen que las autoridades puedan hacer algo en favor de quienes denuncien este tipo de acontecimientos. Solo el 3,9% ha manifestado que han denunciado este tipo de delitos, fundamentalmente porque se trataban de delitos contra el honor de las personas y en favor de proteger la integridad propia de algún familiar.

10. Delitos informáticos más conocidos en el medio

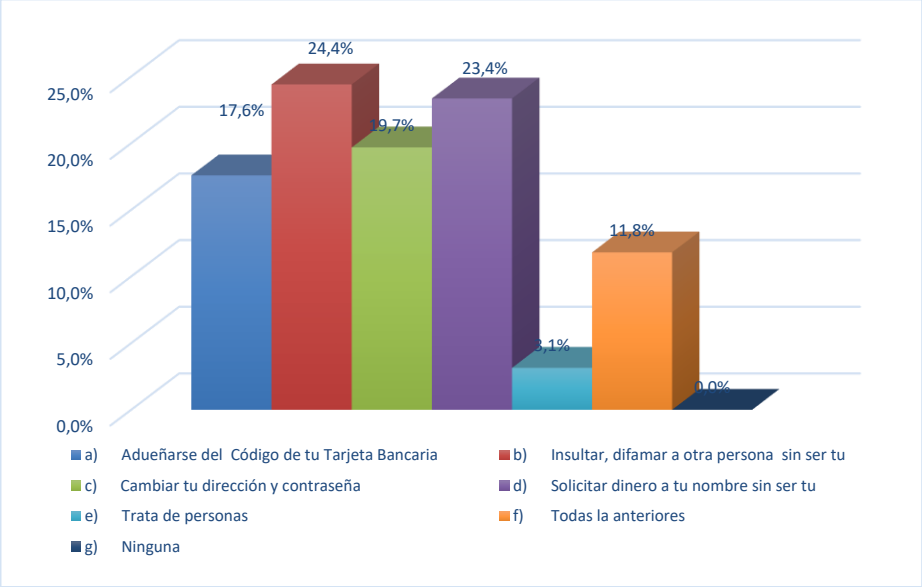
Gráfico 10: Delitos informáticos más conocidos en el medio



En criterio de los participantes de las encuestas realizadas, el delito más frecuente que se comete por medios digitales e internet es el de la pornografía, el 28,3% de los encuestados consideran que esa actividad es la más peligrosa y recurrente en el ámbito nacional; el 24,7 % manifiesta que el delita que con mayor frecuencia se da en medio de la sociedad participante de este estudio es el de la suplantación de identidad (Phishing), este se manifiesta, según los encuestados, en el robo de contraseñas de redes sociales o correos electrónicos, el ingreso indebido a cuentas personales o la suplantación de identidad en las redes sociales a fin de desprestigiar a la persona o engañar a terceros a nombre de la víctima. Otro delito que es considerado relevante en cuanto a la frecuencia en la que se presenta es el del sexting (20,5%), el mismo que consiste en la publicación indebida y no autorizada de imágenes con contenido sexual de terceros sin autorización del propietario, esto se da más entre las parejas sentimentales o entre los menores de edad que sin saberlo comparten imágenes intimas que luego son divulgadas de manera indiscriminada. Entre los delitos mencionados con mayor recurrencia esta también el de la estafa (15,2%), que se da en las redes sociales y ahora en lo que se conoce como las ventas por medio de redes sociales.

11. Consecuencias de la suplantación de identidad informática

Gráfico 11: Consecuencias de la suplantación de identidad informática

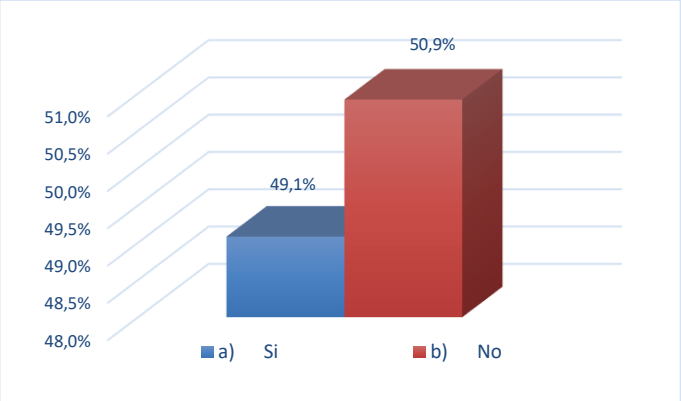


La suplantación de identidad informática, más allá de generar un delito que puede ocasionar la perdida de dinero o de información valiosa para la víctima, también genera algunos conflictos de orden emocional y social, de ahí que algunos autores determinan que este delito puede causar un dolor psicológico real a las víctimas, que pueden sentirse vulnerables, invadidas, traicionadas o avergonzadas en torno al grupo social del que son parte. Esta afirmación es ratificada por los resultados de la encuesta realizada, donde se ha determinado que, según el 24,4% de los participantes la suplantación de identidad (phishing) puede generar la difamación de terceras personas utilizando el nombre o imagen de la víctima. El 23,4 % de los encuestados manifiesta que el phishing es utilizado para solicitar dinero a amigos o familiares a nombre de la víctima (estafa), el 19,7% refiere que el phishing se utiliza más para cambiar contraseñas o acceder de manera ilícita a cuentas tuyas a fin de robar información confidencial; un 17,6% de la población encuestada refiere de que se puede usar este delito para robar el código de acceso a tarjetas bancarias o tner acceso elegal a cuentas financieras de la victioma. De cualquier forma, la población encuestada es consiente de que

el phishing es un delito que genera consecuencias negativas para la victima y por tanto de be ser atendido como un delito informático sancionable en Bolivia.

12. Ha sido víctima de Suplantación de Identidad Informática

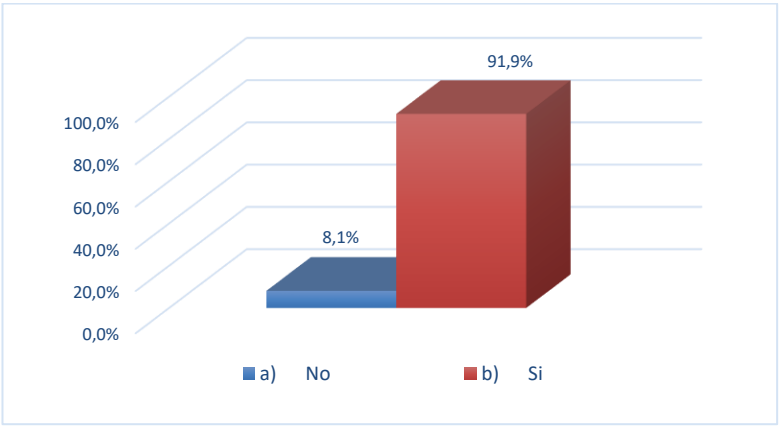
Gráfico 12: Ha sido victimas de Suplantación de Identidad Informática (Phishing)



El 49,1% de los encuestados manifiesta que si han sido victimas en algún momento de suplantación de identidad y robo de contraseñas en algunos medios digitales o redes sociales, el 50,9 % manifiesta no haber tenido este problema.

13. Consideración de si el Phishing puede generar consecuencias graves

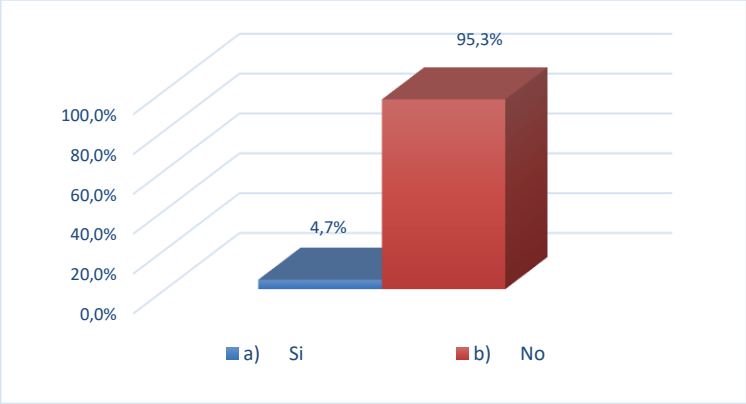
Gráfico 13: Consideración de si el Phishing puede generar consecuencias graves



El 91,9 % de los encuestados manifiestan que el Phishing o suplantación de identidad genera consecuencias graves, entre ellas señalan la posibilidad de perder información confidencial, ser victimas de fraude o perder claves y contraseñas de transacciones financieras que podrían involucrar la perdida de dinero. El 8,1% refiere que no consideran que este delito pueda traer algún tipo de consecuencia grave posterior, en este grupo de personas se encuentran los encuestados más jóvenes.

14. Conocimiento de una norma nacional que sancione el Phishing

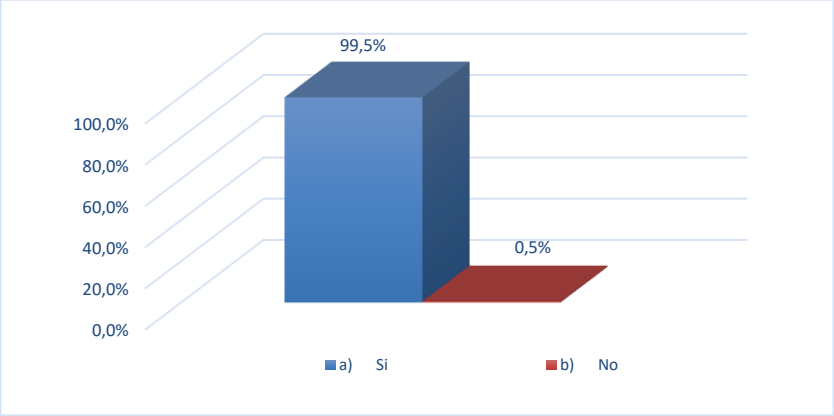
Gráfico 14: Conocimiento de una norma nacional que sancione el Phishing



En Bolivia, el phishing puede ser sancionado como un delito informático según la Ley N° 1390 de Fortalecimiento para la Lucha Contra la Corrupción, que modifica el Código Penal y establece penas de privación de libertad y multas para quienes cometan actos de corrupción que afecten al patrimonio del Estado, incluyendo el uso indebido de sistemas informáticos o telemáticos, pero no lo identifica plenamente como un delito de suplantación de identidad por lo que la población desconoce si este tipo de delitos pueden ser denunciados, así el 95,3 % de los encuestados en este estudio, manifiesta que no conoce de la existencia de una norma específica que sancione el phishing, lo que muestra la necesidad de regular este tipo de actividad delictiva de manera concreta. Solo el 4,7% refiere de que las modificaciones a la normativa penal actual permiten sancionar el delito informático.

15. Debería sancionarse específicamente la suplantación de identidad informática

Gráfico 15: Debería sancionarse específicamente la suplantación de identidad informática



El 99,5 % de los encuestados manifiesta que este delito debe ser identificado y sancionado de manera expresa en la normativa penal boliviana, esto como una forma de resguardo de la actividad realizada por la ciudadanía que utiliza las tecnologías de información y comunicación como parte de su cotidianidad actual. Solo el 5% de los encuestados manifiestan que no es necesario una sanción específica, porque cosieran que de manera general ya la norma nacional sanciona los delitos informáticos y no consideran necesario generar una norma especifica para resguardar a la población boliviana de la suplantación de identidad.

CAPITULO V

CONCLUSIONES

Y

RECOMENDACIONES

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Las conclusiones del presente estudio, se han estructurado en función a los objetivos diseñados inicialmente en el mismo, de manera tal que estos, al ser cumplidos generen las conclusiones que a continuación se detallan:

Primera:

Los parámetros teórico normativos que regulan el derecho a la identidad real y la identidad virtual han permitido definir que, el derecho a la identidad es un derecho humano que implica el reconocimiento de los datos biológicos y culturales que permiten la individualización de una persona como sujeto en la sociedad, este derecho como tal, abarca el derecho a tener un nombre, un apellido, una nacionalidad, a ser inscrito en un registro público como miembro de una familia y de una sociedad.

Así mismo, el derecho a la identidad virtual se refiere al reconocimiento de la persona el ámbito digital, que se construye mediante la interacción social en medios que forman parte de las tecnologías de información y comunicación como las redes sociales, los foros y otras plataformas de uso actual vía internet, pero en la realidad, se ha establecido también que la identidad virtual puede coincidir o no con la identidad real, y puede tener múltiples manifestaciones según el contexto y el propósito de cada persona, en tal contexto la Agencia Española de Protección de Datos, sostiene que el derecho a la identidad digital es una proyección del derecho a la identidad personal en el entorno digital, y que implica el derecho a controlar los datos personales que se generan en ese ámbito; el sociólogo Manuel Castells, afirma que la identidad virtual es una forma de construcción de sentido en un mundo globalizado y diverso, y que puede ser una fuente de empoderamiento, creatividad y participación, es decir que para este autor, la identidad virtual, le permite al individuo elegir la comunidad en la que quiere

participar y la principal motivación de su interés en una o más materias específicas en las que se da cuenta de una identificación y encuentra gente con quien pueda compartir ideas y aficiones pero también abre las puertas a la manipulación social y conflicto de intereses, por lo que se debe regular de manera específica por las sociedades.

El actual Estado Plurinacional de Bolivia se carece de una definición específica de lo que representa la identidad virtual y por tanto la suplantación de la misma puede ser considerada porco importante generando espacios para la comisión de delitos que perjudiquen el desenvolvimiento del individuo y de la comunidad.

Segunda:

Al analizar las bases jurídicas que definen la figura penal de la suplantación de identidad como delito informático, se ha podido llegar a la siguiente conclusión, la suplantación de identidad es un delito en el que el infractor se hace pasar por otra persona para obtener algún beneficio ilícito, como acceder a sus datos personales, financieros, bancarios o de clientes, o dañar su reputación, honor o intimidad, esta suplantación de identidad puede realizarse mediante el uso de correos electrónicos, mensajes, sitios web o perfiles falsos que imitan a entidades o personas legítimas, ninguna de estas dos figuras esta establecida de manera especifica en la legislación boliviana.

La figura de suplantación de identidad propiamente dicha, no está regulada de manera específica en la legislación boliviana, siendo sus proximidades más cercanas las figuras de la falsedad material, tipificada por el artículo 198 del Código Penal, y la falsedad ideológica, tipificada por el artículo 199 del mencionado código. En consecuencia, la suplantación de identidad informática no se ha considerado, todavía, dentro de la norma boliviana, lo más cercano a esta figura es la referencia al delito informático establecido en la Ley N° 1768 de Modificaciones al Código Penal que incorpora el artículo 363 bis la Manipulación Informática definida como el procesamiento o transferencia de datos informáticos

que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto; esta misma norma incorpora el articulo 363 ter referido a la Alteración, Acceso y Uso Indebido de Datos Informáticos almacenados en una computadora o en cualquier soporte informático que ocasione al titular de la información; ninguno de estos dos “nuevos” artículos define claramente la suplantación de identidad que no considera, por ejemplo, la comisión de otros delitos, como estafa, amenaza, injuria, calumnia, falsedad o chantaje que debían ser atendidos por la norma especifica

Lo expuesto permite establecer que existe una necesidad, que fundada en la cotidianidad actual del crecimiento del uso de redes sociales y medios digitales, de regular la suplantación de identidad de manera expresa como garantía para poder salvaguardar los derechos de los ciudadanos bolivianos y e garantizar el correcto relacionamiento social de estos por los medios digitales que son parte de la actual tecnología de información y comunicación en la que se vive y que obliga a la normativa a adecuarse a estos cambios de conducta motivados por la modernidad.

Tercera:

Al estudiar las implicancias sociales y jurídicas que causa la suplantación de identidad como delito informático en la población boliviana, luego de un somero análisis conceptual doctrinario y jurídico cumple su principal objetivo planteado presentar al tribunal el anteproyecto de ley para modificar el Artículo 363 de nuestro Código Penal Boliviano para incorporar al mismo el delito de suplantación de identidad electrónica como delito informático.

Ahora, la suplantación de identidad informática, es algo novedoso y nace con los avances tecnológicos y actualmente no es parte de la norma penal lo que facilita la impunidad de los infractores y fomenta la pasividad de una sociedad que no conoce cuales son los alcances legales para poder proteger su derecho a la identidad tanto real como virtual.

El Estado boliviano comienza a introducirse a la época de digitalización o y biometrización el cual consiste en el registro de las huellas dactilares y la captura de los rasgos faciales de forma digital, que permite al SEGIP y otras instituciones generar bases de información con los datos personales de la comunidad, por medio de estas instituciones se garantiza la seguridad de esta información , este actuar es parte del proceso obligatorio e imprescindible para recabar cualquier documento de identidad en muchos casos.

En este aspecto, Bolivia es un estado vulnerable ante el crimen informático; esto se debe al gradual crecimiento del número de actividades que participan directamente de las tecnologías de información y comunicación, al punto de depender de su seguridad y eficiencia como en el caso de la banca, cuyas transacciones, depósitos y retiros, son administrados por equipos de computación, que deben contar con sistemas informáticos seguros para resguardar la información contenida en ellos. Toda esta situación novedosa exige, la seguridad de los sistemas de comunicación y su protección contra el crimen informático, aspecto que no es posible dada la inexistencia de norma especifica que regule la suplantación de identidad como delito informático.

La falta de sanciones efectivas contra el delito denominado phishing tiene diversas consecuencias negativas para la sociedad, así, este delito genera pérdida de datos personales y financieros, ya que los delincuentes se hacen pasar por entidades legítimas para obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales de las víctimas, que al no identificarse claramente, hace que las personas pueden ser más susceptibles a caer en estas trampas y perder sus datos, lo que puede llevar a robos de identidad, fraude financiero y otros tipos de delitos.

Por otro lado el phishing puede tener un impacto significativo en la economía, puesto que este delito no alcanza solo a personas naturales, las empresas y organizaciones son vulnerables también a estos ataques, y si no se sancionan, pueden sufrir pérdidas financieras importantes, orillándolos, en base al engaño y la utilización fraudulenta de identidades, a realizar transacciones no autorizadas o a revelar información financiera sensible, lo que puede generar costos

significativos para las instituciones financieras. En esa misma lógica, la suplantación de identidad digital, socava la confianza de las personas en el entorno digital, si no se sanciona debidamente, puede generar una sensación de inseguridad y desconfianza generalizada hacia las transacciones en línea y las comunicaciones electrónicas lo que detendría el avance y .el crecimiento del comercio electrónico y obstaculizar el desarrollo de la sociedad como tal.

5.2. RECOMENDACIONES

Primera:

Los adelantos tecnológicos y el crecimiento del uso de las redes sociales y los medios digitales, establecen una necesidad de generar legislación acorde a la realidad que vive la sociedad, por lo que se recomienda, implementar legislación y regulaciones específicas y dinámicas que puedan adecuarse a los contextos actuales en los que se desarrolla la sociedad; los gobiernos deben establecer leyes y regulaciones claras que penalicen el phishing y otros delitos cibernéticos de manera específica. Estas leyes deben tener sanciones adecuadas y disuasorias para los infractores, incluyendo multas y penas privativas de libertad que desalienten a los ciudadanos a incurrir en estos delitos. Paralelamente a estas normas reguladoras, se recomienda que el estado como tal refuerce la seguridad informática, logrando que las organizaciones o instituciones tanto públicas y privadas puedan implementar y garantizar a los usuarios o ciudadanos medidas de seguridad cibernética robustas para prevenir el phishing y la perdida de información digital, esto puede incluir sistemas de detección de intrusiones, autenticación de dos factores, filtros de correo electrónico y programas de seguridad actualizados. Además, es importante mantener al día los sistemas y aplicaciones con actualizaciones de seguridad fundamentalmente en el ámbito público para que lo obsoleto de los sistemas actuales no se constituyan en factores de riesgo de pérdida de información.

Segunda:

Es necesario recomendar a las organizaciones estatales que fortalezcan la cooperación internacional, esto en la medida de que el phishing y otros delitos informáticos, son un problema global que trasciende las fronteras, la versatilidad del manejo de internet que, además, tiene la particularidad de romper barreras de tiempo y distancia, hacen que la detección delictiva sea más difícil, más si no existe una cooperación multilateral entre los países para lidiar con este tipo de delincuencia. Es importante fomentar la cooperación internacional entre los países para investigar y sancionar a los perpetradores del phishing y en esto se debe incluir el intercambio de información, la colaboración en investigaciones conjuntas y la extradición de los delincuentes.

En esa lógica se debe fomentar la colaboración entre sectores del Estado, el combate a la suplantación de identidad en específico y del delito informático en general, requiere una colaboración efectiva entre los sectores público y privado. Las empresas, proveedores de servicios de Internet, instituciones financieras y organismos gubernamentales deben trabajar juntos para compartir información sobre amenazas, intercambiar mejores prácticas y colaborar en la lucha contra el delito informático. Paralelamente la educación y la concienciación son fundamentales para prevenir este delito, en esa lógica, se recomienda también que, las empresas, organizaciones y gobiernos deben invertir en programas de capacitación para enseñar a los usuarios a identificar y evitar los ataques cibernéticos, es decir que se recomienda que, los usuarios deben ser informados en temáticas que expliquen las tácticas utilizadas por los estafadores y las mejores prácticas para proteger su información personal.

Tercera:

Así mismo se recomienda que las autoridades tanto gubernamentales y policiales deben establecer mecanismos de denuncia y respuesta oportuna, es decir, es importante que las víctimas de phishing tengan mecanismos efectivos para denunciar los ataques y recibir apoyo oportuno para poder ser escuchados, así, las autoridades deben establecer canales de denuncia adecuados y responder

de manera rápida y eficiente a las denuncias para investigar y sancionar a los perpetradores.

Cuarta:

Finalmente se recomienda actualizar regularmente la legislación y las estrategias de prevención que asuma el estado y la entidad policial, esto en la medida de que el crecimiento de la ciberdelincuencia está en constante evolución, por lo que es importante que las leyes y estrategias de sanción y prevención del phishing se actualicen regularmente para hacer frente a las nuevas amenazas y tácticas utilizadas por los delincuentes en resguardo de la ciudadanía y su seguridad real y virtual.

.

CAPITULO VI

PROPUESTA

PROPUESTA

4.1 ÁMBITO GEOGRÁFICO DE APLICACIÓN DEL PROYECTO DE LEY

La presente propuesta por el carácter de cobertura que tiene y la norma específica propuesta, debe tener un carácter de implicación nacional, sin afectación a la condición de gobierno autónomo que tienen los municipios y los departamentos del Estado Plurinacional de Bolivia.

4.2. FORMULACIÓN DE LA NORMA

La propuesta de la presente investigación se formula en calidad de Ante Proyecto de Ley, la misma que podrá ser considerada por el ente legislador como iniciativa ciudadana.

EXPOSICIÓN DE MOTIVOS

El presente Ante proyecto de Ley se plantea realizar las adecuaciones, modificaciones e incorporaciones necesarias al Código Penal sobre los nuevos delitos informáticos que se presentan en el desarrollo social de la comunidad como producto del uso de las tecnologías de información y comunicación en la actualidad las mismas que generan que los delitos mutan y se perfeccionan día a día a la par del avance tecnológico.

En líneas generales, al hablar de delitos informáticos la ley se refiere a aquellas conductas indebidas e ilegales en las que interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo. Los delitos informáticos son entendidos respecto al lugar que ocupa la tecnología para la comisión del hecho ilícito más que a la naturaleza delictiva del acto mismo, ya que casi todos los delitos contemplados en los ordenamientos jurídicos locales pueden cometerse a través de un dispositivo informático.

En base a ello, se incorpora como objeto del presente Ante proyecto la regulación de los mecanismos que garanticen la prevención y sanción de todo acto considerado suplantación de identidad informática, entendiendo por suplantación de identidad informática es un delito que consiste en hacerse pasar por otra persona para obtener algún beneficio ilícito, como acceder a sus datos personales, financieros, bancarios o de clientes, o dañar su reputación, honor o intimidad.

Se propone un cambio de paradigma en la materia y la normativa existente en este ámbito, la cual sólo apuntaba a la criminalización e imposición de penas para los autores de los delitos establecidos o que se buscaban establecer en las legislaciones internas. A tal fin se implementa como objetivo central “la prevención ciudadana”, específicamente orientada a todos los usuarios de redes sociales, medios digitales y otras plataformas que en base al uso del internet y la comunicación sirven para la transmisión y almacenaje de información personal y confidencial de un ciudadano.

Se introducen la identificación plena de la suplantación de identidad virtual que ayudan a hacer completa la modificación propuesta y se redefinen conceptos ya existentes adecuándolos a la actualidad

Finalmente, se propone la modificación del Código Penal y las conductas descritas como delitos y se incorpora la identificación de la suplantación de identidad (phishing), actualizando el accionar delictivo que se va perfeccionando para no ser alcanzadas por las normas y ello impone el desafío de ir readecuando las herramientas penales para su persecución y sanción.

Así, se propone sancionar aquellas conductas relacionadas al delito informático destacando sus alcances y conductas relacionadas con delitos conexos al mismo tales como, el fraude, la difamación.

Por lo expuesto, el presente Ante proyecto de Ley busca, la prevención de los delitos informáticos que permite armonizar respuestas o soluciones conjuntas ante temas que requieren de la intervención de los actores fundamentales del

cumplimiento de la ley para la adecuación normativa capaz de combatir de manera efectiva los delitos actuales que nacen del avance de la sociedad.

PROBLEMÁTICA

No obstante, al régimen de lo establecido por la Constitución Política del Estado, la Ley N° 1768 de modificaciones al Código Penal, a la fecha no ha definido de manera clara y precisa el delito de suplantación de identidad informática (phishing), lo que impide que se pueda sancionar los intentos de delincuentes de apoderarse de manera indebida de la información personal e identificativa de los ciudadanos habitantes y estantes del Estado Plurinacional de Bolivia, lo que genera que el ciudadano común desconozca la forma de denuncia de este tipo de delitos.

Esta situación no solo genera inseguridad en las relaciones sociales generadas entre los ciudadanos que utilizan los medios digitales como vía de transmisión de comunicación e información por medios digitales y/o redes sociales.

Ahora, la carencia de una sanción a un tercero que acceda a información personal no autorizada y el uso de la misma no se a definido de manera clara en la normativa boliviana; el art. 363 ter actual, identifica solo el a datos informáticos como motivo de delito, y no identifica que este agresor pueda suplantar la identidad del usuario por medio de este acceso y a partir de esta suplantación pueda cometer otro delito tal como la estafa.

PROPUESTA

En virtud a todo lo expuesto sin desconocer los avances legislativos realizados en mérito de adecuar la normativa nacional al contexto actual de avance tecnológico realizado por la Ley N° 1768 de Modificaciones al Código Penal que define los Delitos Informáticos, considerando los parámetros técnicos que deberán tomar en cuenta los legisladores para definir el delito informático de la suplantación de identidad y su sanción específica se propone, un anteproyecto

de ley en beneficio a las necesidades de los usuarios de redes sociales y medios digitales que comparten información y comunicación en el territorio nacional, de la siguiente manera:

PROYECTO DE LEY

LA ASAMBLEA LEGISLATIVA PLURINACIONAL

DECRETA:

ARTÍCULO PRIMERO.- Se incluye el articulo 363 quater en el Capítulo XI Delitos Informáticos del Código Penal Boliviano modificado en aplicación del artículo 2, numeral 57 de la Ley 1768 del 10 de marzo de 1997, con el tenor siguiente:

" Artículo 363 quater (SUPLANTACIÓN DE IDENTIDAD, ROBO Y ESTAFA POR VÍA INFORMÁTICA)

Se define a la suplantación de identidad por vía informática al delito que consiste en que una persona utilice deliberadamente y sin autorización la identidad de otra persona a fin de obtener algún beneficio ilícito, como acceder a sus datos personales, financieros, bancarios o de clientes, o dañar su reputación, honor o intimidad. La suplantación de identidad puede realizarse mediante el uso de correos electrónicos, mensajes, sitios web o perfiles falsos que imitan a entidades o personas legítimas.

En consecuencia, se sanciona la suplantación de identidad por vía informática con reclusión de uno a cuatro años cuando:

1. El que, con intención de obtener un beneficio o con el fin de afectar la imagen y dignidad de la víctima utilice sistemas informáticos para suplantar la identidad de una persona sea natural o jurídica generándole perjuicio con la perdida total o parcial de la información propia del titular.

2. El que cometiere, suplantación de identidad, mediante la utilización de tecnología informática o a través de un medio de comunicación, con la intención de generar calumnia, actos deshonestos o difamación mellando la reputación, honor o derecho a la intimidad de la victima

3. El que por medio de la suplantación de identidad cometa estafa informática, financiera o reciba dinero o beneficio económico doloso a nombre de la víctima

4. El que, con intención de alterar contenidos de un mensaje de datos informáticos o electrónicos de empresas públicas o privadas ingrese a los sistemas informáticos de las mismas suplantando la identidad de la víctima.

5. El que apropiándose de accesos y códigos personales e íntimos suplante la identidad de la víctima y acceda a información de correos electrónicos, conversaciones privadas y las publique para desacreditar al titular.

El delito se agravará en los casos que se cometa en contra o sean víctimas de las consecuencias de los actos delictivos menores de 6 a 14 años de edad y esta será sancionada con reclusión de cuatro a diez años de presidio.

BIBLIOGRAFÍA

Alimena, B. (1915). *Principios de Derecho Penal.* España: Nuevo mundo .

Atheniense, A. (2012). *Auto-Aplicaçao do Código do Consumidor Brasileiro nas Transaçoes de Bens Corpóreos pelo Comércio Eletrônico na Internet.* Chile: III Congreso de Derecho Informático.

BBVA. (1 de enero de 2020). *Ciberataques: objetivo, tipos y medidas para protegerse*. Obtenido de Banco BBVA: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/ciberataques-objetivo-tipos-y-medidas-para-protegerse.html

BCN Chile. (23 de junio de 2022). *Delitos Informáticos, Sistemas de Información, Ley no. 19.223.* Obtenido de Biblioteca Central de la Nación: https://www.bcn.cl/leychile/navegar?idNorma=30590&idParte=

Beling, E. (2002). *Esquema de Derecho Penal.* Argentina: Librería "El Foro".

Belisario, A. (2018). *Análisis de métodos de ataques de phishing.* Argentina: Universidad de Buenos Aires.

Betancourt López, E. (1994). *Teoria Del Delito.* México: Editorial Porrúa. S.A.

Borja, J. (15 de junio de 2021). Guía rápida para protegerse del robo de identidad. *ABC Sociedad*.

Cabanellas De Torres, G. (2000). *Diccionario jurídico y social.* Heliasta.

Calderon, D. (2021). *Fraude y delito informatico*. Obtenido de Calameo: https://www.calameo.com/books/0043912194c9029c11cbc

Callegari, N. (1985). Delitos informáticos y legislación. *Revista de la Facultad de Derecho y Ciencias Políticas - Colombia*, 112 - 118.

CEA. (12 de abril de 2018). *La protección de los datos personales en la constitución.* Obtenido de Confederación de Empresarios de Andalucia : https://www.cea.es/portal/novedades/2010/guias/ProteccionDatosEmpresa/1_1.htm

Collado, J. (14 de Mayo de 2018). *Delitos Informáticos en el Código Penal del Estado.* Obtenido de Poder Judicial Michoacan: https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap3.htm

Cuello, E. (2004). *Derecho Penal I.* España: Bosch.

Felipe, C. (2020). *¿Qué es la doctrina jurídica?* Obtenido de FC Abogados: https://fc-abogados.com/es/que-es-la-doctrina-juridica/#:~:text=La%20doctrina%20estudia%20los%20manantiales,significado%20de%20los%20modelos%20jur%C3%ADdicos.

Fricke, M. (2010). Autoconciencia e identidad personal. *Península*, 99-118.

Gaceta Oficial de Bolivia. (2009). *Constitución Política del Estado.* Bolivia: Gaceta Oficial de Bolivia.

Garrido, M. (2005). Derecho Penal. *Revista chilena de Derecho y Tecnología*.

González de la Vega, F. (1996). *Derecho Penal Mexicano.* México: Editorial Porrúa.

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la Investigación.* México: McGraw-Hill.

Hernandez, S., Fernández, C., & Baptista, L. (2014). *Metodología de la Investigación Cietífica, Sexta edición.* México: McGraw Hill.

Herrera, R. (2004). *El Derecho en la Sociedad de la Información: Nociones generales sobre el Derecho de las Tecnologías de la Información y las*

Comunicaciones. Obtenido de Derecho Tecnológico: http://www.derechotecnologico.com/estrado/estrado002.html

Jakobs, G. (1997). *Derecho Penal.* España: EDICIONES JURIDICAS, S. A.

Jimenez De Asua, L. (2018). Principios del Derecho Penal. La Ley el Delito. En G. Rosas, *Los Derechos del Inimputable Penal* (pág. 3). Perú: Revista Postgrado Scientiarvm, Universidad Catolica de Santa María.

Kaspersky. (28 de julio de 2020). *¿Qué es la ciberseguridad?* Obtenido de Karspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Levene, R., & Chiavalloti, A. (2019). *Delitos Informáticos.* México: VI Congreso Iberoamericano Derecho e informática.

Listz, F. (1999). *Tratado De Derecho Penal.* España: Editorial Reus.

Luna, P. (23 de febrero de 2021). *Política criminal.* Obtenido de Foro Juridico México: https://forojuridico.mx/politica-criminal/#:~:text=La%20pol%C3%ADtica%20criminal%20consiste%20en,del%20delito%20y%20acciones%20de

Mostajo, M. (2015). *Seminario Taller de Grado.* La Paz- Bolivia: Castillo Impresores.

Novoa, E. (2000). *Curso de Derecho Penal Chileno.* Chile: Editorial Jurídica de Chile.

Núñez Ponce, J. (2007). Perspectivas del derecho informático, comercio electrónico e internet en el Perú. *Ius Et Praxis*, 59-77.

OEA. (2001). *Convenio Sobre la Ciberdelincuencia.* Obtenido de Organizaciín de los Estados Amerícanos : https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

ONU. (2009). *La Declaración Universal de Derechos Humanos*. Obtenido de Naciones Unidas: http://www.un.org/es/universal-declaration-human-rights/

OSI. (2022). *Guía de ciberseguridad. La ciberseguridad al alcance de todos.* España: Ministerio de Asuntos Económicos y Transformación Digital.

Ossorio, M. (1990). *Diccionario de ciencias jurídicas, políticas y sociales.* Argentina: Heliasta S.R.L.

Pessó, A. (2015). *Usurpación de identidad en las redes sociales: facebook y twitter. Tratamiento legal y jurisprudencial en Chile .* Chile: Universidad de Chile.

Rendon, D. (2012). *La eficacia de la prueba digital en el proceso penal colombiano.* Colombia: Universidad De Medellin.

Rimber, J. (2 de diciembre de 2018). *Delito Suplantación identidad*. Obtenido de Rinber Abogados: https://www.rinberabogados.com/areas-de-penal/delito-suplantacion-identidad/#:~:text=Se%20entiende%20por%20suplantaci%C3%B3n%20de,realizar%20ataques%20contra%20terceras%20personas.

Rodríguez, F. (2012). *Nuevos delitos informáticos.* España: DOCT.

Rosado, J. (2020). *Bolivia sumó 250.000 usuarios en las redes sociales en el último año*. Obtenido de Economy.com: Bolivia sumó 250.000 usuarios en las redes sociales en el último año

Sarzana, C. (2019). Criminalità e tecnologia en computers crime. rassagna penitenziaria e criminologia. En M. Estrada, *Delitos informáticos.* México: Universidad Abierta.

Téllez, J. (2005). *Derecho Informatico 2da. Edicicón.* Mexico: McGraw Hill.

Toffer, A. (2000). *El Schok del Futuro.* España: Plaza & Janes S.A. .

UNODC. (2004). *Convención de las Naciones Unidas .* EE.UU. : Naciones Unidas .

Vargas Flores, A. (2007). *Guía teórico practico, para la elaboración de Tesis.* La Paz Bolivia: Edit. Juventud.

Vargas Flores, A. (2012). *Guía teórico practico, para la elaboración de Tesis.* La Paz Bolivia: Edit. Juventud.

Zaffaronni, E. (1999). *Tratado de Derecho penal, Parte General.* Argentina: Edar.

ANEXOS

ANEXOS

Anexo No. 1: Formulario de Encuesta

ENCUESTA

La presente encuesta tiene fines de recopilación de información que será utilizada en la elaboración de un estudio académico titulado: “Inserción de la figura penal de suplantación de identidad como delito informático en el Art. 363 del Código Penal”, el mismo que será presentado a la Universidad Mayor de San Andrés, por lo que los datos recabados por la misma serán utilizados de manera confidencial. Rogamos la mayor veracidad posible en las repuestas emitidas.

INSTRUCCIONES.

Revise detenidamente las preguntas y seleccione la respuesta marcando la opción elegida con una (X) en el espacio reservado. Rogamos a usted llenar el formulario con la mayor claridad y objetividad posible.

I. DATOS GENERALES

1. Género:
    a) Femenino .....
    b) Masculino .....
2. ¿En qué rango de edad se encuentra actualmente?
    a) 18 a 22 años .....
    b) 23 a 28 años .....
    c) 29 a 46 años .....
    d) 47 a 59 años .....
    e) 60 y más años .....
3. ¿Cuál es su estatus social actualmente?
    a) Soltero (a) sin hijos .....
    b) Soltero (a) con hijos
    c) Casado (a) sin hijos .....
    d) Casado (a) con hijos

e) En unión libre sin hijos
f) En unión libre con hijos .....

4. Actualmente ¿Cuál es el grado mayor de educación y/o profesionalización que ha alcanzado?
    a) Bachillerato inconcluso .....
    b) Bachillerato concluido .....
    c) Formación técnica inconclusa .....
    d) Formación técnica concluida .....
    e) Licenciatura inconclusa .....
    f) Licenciatura concluida .....
    g) Post Grado inconcluso .....
    h) Post Grado concluido .....
5. ¿A cuál de los siguientes rangos pertenece el monto que usted percibe al mes por su trabajo, actividad o negocio?
    a) Menos de Bs 2.000 .....
    b) De Bs 2.000 a Bs 3.000 .....
    c) De Bs 3.001 a Bs 4.000 .....
    d) De Bs 4.001 a Bs 7.000 .....
    e) De Bs 7.001 a Bs 13.000 .....
    f) Más de Bs 13.000 .....

II. UTILIZACIÓN DE MEDIOS DE COMUNICACIÓN DIGITAL

6. ¿Utiliza el correo electrónico u otros medios digitales como las redes sociales para comunicarse con su entorno?
    a) Si .....
    b) No .....
7. ¿Con que frecuencia utiliza estos medios digitales de comunicación?
    a) Una vez a la semana .....
    b) Todos los días .....
    c) Una vez al mes .....
    d) Casi nunca .....
8. ¿Toma alguna precaución especial para cuidar sus contraseñas de acceso a los medios informáticos de comunicación?
    a) No .....
    b) Si ..... ¿Indique Cuál? .....

9. ¿Alguna vez ha sido víctima de un acceso indebido o de terceras personas a sus cuentas de correo o de redes sociales?
    a) Si .....
    b) No .....

10. ¿Ha denunciado ante alguna autoridad el hecho de que le hayan abierto o utilizado sus correos o redes sociales sin su autorización
    a) Si .....
    b) No ..... ¿Por qué? .....

III. DELITO INFORMÁTICO

11. ¿Cuáles de los siguientes delitos informáticos cree que es el más común en el medio ?
    a) Sexting (enviar fotos, videos o mensajes de contenido sexual) .....
    b) Pornografía .....
    c) Ciberacoso .....
    d) Phishing (Suplantación de identidad) .....
    e) Estafas .....
    f) Filtración de material sexual (mío o de un tercero) .....
    g) Acceso a datos personales .....
    h) Revelación de secretos .....
    i) Otro ..... ¿Indique cuál? .....

12. ¿Cuál crees que es la consecuencia más común de la suplantación de identidad informática?
    a) Adueñarse del Código de tu Tarjeta Bancaria y realizar transacciones sin tu autorización .....
    b) Insultar, difamar a otra persona por las redes sociales sin ser tu .....
    c) Cambiar tu dirección y contraseña de tus redes sociales y evitar tu manejo .....
    d) Solicitar dinero u otras dadivas a tu nombre sin ser tu .....
    e) Trata de personas .....
    f) Todas la Anteriores .....
    g) Ninguna .....

13. ¿Has sido víctima alguna vez de la suplantación de identidad en las redes sociales o en medios electrónicos?
    a) Si .....
    b) No .....

14. ¿Considerada que el Phishing (Suplantación de identidad) es un delito que puede traer consecuencias graves?
    a) No .....
    b) Si ..... ¿Indique Cuáles? .....
15. ¿Sabe de alguno norma nacional que sancione el Phishing (Suplantación de identidad) como un delito informático?
    a) Si .....
    b) No .....
16. En tu criterio, debería sancionarse drásticamente este tipo de acciones que atentan contra la identidad de las personas
    a) Si .....
    b) No .....

Gracias por tu Participación…

Anexo No. 2 Glosario De Términos

ACTIVO PATRIMONIAL: Conjunto de bienes y derechos que integran el haber de una persona física o jurídica.

BASEDEDATOS: Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.

BROWSER (BUSCADOR): El software para buscar y conseguir información de la red WWW. Los más comúnmente usados son Microsoft Explorer, Firefox y Opera.

COOKIE: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que está haciendo. Hay una variedad de "anti-cookie" software que automáticamente borra esa información entre visitas a su sitio.

DIALUP (MARCAR): El método de conectarse con Internet vía la línea de teléfono normal mediante un modem, en vez de mediante una LAN (Red Local) o de una línea de teléfono alquilada permanentemente. Esta es la manera más común de conectarse a Internet desde casa si no ha hecho ningún arreglo con su compagina de teléfono o con un ISP. Para conexiones alternativas consulte con su ISP primero.

DIGITAL SIGNATURE (FIRMADIGITAL): El equivalente digital de una firma autentica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma escribió o autorizo el Archivo.

DOCUMENTOELECTRÓNICO: Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles de HTTP (HYPER TEXT TRANSPORT PROTOCOL): El conjunto de reglas que se usa en Internet para pedir y ofrecer páginas de la red y demás información. Es lo que pone al comienzo de una dirección, tal como "http: /," para indicarle al buscador que use ese protocolo para buscar información en la página.

INTERNET SERVIC EPROVIDER(ISP)(PROVEEDOR DE SERVICIO DE INTERNET) Una persona, organización o compagina que provee acceso a Internet. Además del acceso a Internet, muchos ISP proveen otros servicios tales como anfitrión de Red, servicio de nombre, y otros servicios informáticos.

MENSAJE DE DATOS: Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.

MODEM: Un aparato que cambia datos del computador a formatos que se puedan transmitir más fácilmente por línea telefónica o por otro tipo de medio.

SISTEMA TELEMÁTICO. Conjunto organizado de redes de telecomunicaciones que sirven para trasmitir, enviar, y recibir información tratada de forma automatizada.

SISTEMA DE INFORMACIÓN: Se entenderá como sistema de información, a todo sistema utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma de mensajes de Datos SISTEMA INFORMÁTICO: Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.

SOCIEDAD DE LA INFORMACIÓN: La revolución digital en las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de información, ideas y conocimientos en todo el planeta. Ha causado una

impresión profunda en la forma en que funciona el mundo. La Internet se ha convertido en un recurso mundial importante, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial, como para el mundo en desarrollo por su función de pasaporte para la participación equitativa y para el desarrollo económico, social y educativo.

SOPORTE LÓGICO: Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que pueden ser empleados para registrar información en un sistema informático.

SOPORTE MATERIAL: Es cualquier elemento corporal que se utilice para registrar toda clase de información.

TELEMÁTICA: neologismo que hace referencia a la comunicación informática, es decir la transmisión por medio de las redes de telecomunicaciones de información automatizada.