UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

USURPACIÓN DE IDENTIDAD PERSONAL POR MEDIOS INFORMÁTICOS EN EL TERRITORIO GUATEMALTECO

ASTRID MARISSA JEREZ JUÁREZ

GUATEMALA, MAYO DE 2024

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIA JURÍDICAS Y SOCIALES

USURPACIÓN DE IDENTIDAD PERSONAL POR MEDIOS INFORMÁTICOS EN EL TERRITORIO GUATEMALTECO

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

ASTRID MARISSA JEREZ JUÁREZ

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, mayo de 2024

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	M. Sc.	Henry Manuel Arríaga Contreras
VOCAL I:	Licda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Rodolfo Barahona Jácome
VOCAL III:	Lic.	Helmer Rolando Reyes García
VOCAL IV:	Br.	Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br.	Gustavo Adolfo Oroxom Aguilar
SECRETARIO:	Lic.	Wilfredo Eliú Ramos Leonor

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas en la tesis". (Artículo 43 de Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Públ

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 10 de mayo de 2018.

Atentamente pase al (a) Profesional, **MIRIAM YOLANDA NAJARRO LÓPEZ**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **ASTRID MARISSA JEREZ JUÁREZ**, con carné **201211375**, intitulado **USURPACIÓN DE IDENTIDAD PERSONAL POR MEDIOS INFORMÁTICOS EN EL TERRITORIO GUATEMALTECO.**

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

LIC. ROBERTO FREDY ORELLANA MARTÍNEZ
Jefe(a) de la Unidad de Asesoría de Tesis

Fecha de recepción 12 / 05 / 2018 f) _____
Asesor(a)
(Firma y Sello)
Miriam Yolanda Najarro López
ABOGADA Y NOTARIA

Licda. Miriam Yolanda Najarro López
Abogada y Notaria

Guatemala, 28 de octubre de 2021

Doctor
Carlos Ebertito Herrera Recinos
Jefe de la Unidad de Asesoría de Tesis
Universidad de San Carlos de Guatemala
Facultad de Ciencias Jurídicas y Sociales.

Estimado Doctor:

Me es grato presentarle para su aprobación definitiva como requisito final para optar al título de Licenciada en Ciencias Jurídicas y Sociales, Abogada y Notaria, el trabajo de tesis de la Bachiller **Astrid Marissa Jerez Juárez** cuyo tema es **"USURPACIÓN DE IDENTIDAD PERSONAL POR MEDIOS INFORMÁTICOS EN EL TERRITORIO GUATEMALTECO."**, el cual cumple apropiadamente con los requisitos académicos exigidos por esa tricentenaria casa de estudios.

De conformidad con el articulo número treinta y uno (31) del normativo para la elaboración de tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, como asesora de tesis emito dictamen correspondiente y hago constar mi opinión respecto a: **I)** Del contenido científico y técnico: si se cumple con el plan de trabajo aprobado en todo su contenido tanto científico, como las técnicas utilizadas; **II)** De la metodología y técnicas de investigación utilizadas en el presente trabajo manifiesto que se usó el método científico, el método deductivo y método inductivo; y se uso como técnica de investigación la bibliográfica; **III)** La redacción de la tesis, si cumple hay coherencia, relación, conexión, y concordancia,

además cumple con requisitos de forma y ortografía; **IV)** Cuadros estadísticos no fueron necesarios; **V)** De la contribución científica, la tesis de la bachiller Jerez Juárez es un interesante aporte investigativo que demuestra que, con la voluntad política apropiada las autoridades legislativas del país pueden impulsar y aprobar un proyecto de ley para la penalización del delito de usurpación de identidad personal por medios informáticos en Guatemala, quedando demostrado el vacío legal que limita la aplicación y la sanción por este tipo de ilícito penal. **VI)** La Conclusión Discursiva, demuestra que el Código Penal de Guatemala que está vigente actualmente contiene un apartado de delitos informáticos, pero no incluye a la usurpación de identidad personal por medios informáticos como un delito, por lo que se hace necesario brindarle protección y seguridad informática a la sociedad guatemalteca, y solucionar el problema de falta de regulación legal de este ilícito. **VII)** La bibliografía utilizada, fue suficiente, toda vez que se enriqueció con libros de texto, leyes y compendios literarios nacionales y se utilizo el derecho comparado, por lo que hay suficiente fundamento teórico en el trabajo.

Por lo tanto, se aprueba el trabajo de investigación, toda vez que cumple con los requisitos exigidos por esta casa de Estudios. También declaro expresamente que no hay parentesco dentro de los grados de ley con la estudiante.

Atentamente,

Miriam Yolanda Najarro López
ABOGADA Y NOTARIA

Licda. Miriam Yolanda Najarro López
Abogada y Notaria.
Oficina 913 Torre Profesional II, 6ª. Ave. 0-60 zona 4
Ciudad Guatemala. C.A.
Tel. 23352585 - 52049881 Miriam_askr@hotmail.com

D.ORD. 264-2024

Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, trece de marzo de dos mil veinticuatro.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante, **ASTRID MARISSA JEREZ JUÁREZ,** titulado **USURPACIÓN DE IDENTIDAD PERSONAL POR MEDIOS INFORMÁTICOS EN EL TERRITORIO GUATEMALTECO.** Artículos 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

HMAC/JIMR

DEDICATORIA

A MI PADRE CELESTIAL: Por ser mi creador, acompañarme en cada momento de mi vida y llenarla de bendiciones.

A MIS PADRES: Juan Carlos Jerez Ortíz y Sandra Alicia Juárez Sánchez, por su amor, dedicación, entereza, sacrificio, paciencia y entrega, y por su total apoyo para lograr mis metas a lo largo de mi vida.

A MI ESPOSO: José Gerardo García Pineda, por su infinito amor, apoyo y comprensión, por ayudarme y motivarme a cumplir mis deseos y metas, por ser la luz que ilumina mi vida y ser ejemplo de persona.

A MIS HERMANOS: Juan Carlos y Sandra Karinna Jerez Juárez, por ser un ejemplo y guía para ser mejor, por estar presentes en cada momento y ser un segundo padre y una segunda madre en mi vida.

A MIS SUEGROS Y CUÑADOS: Por sus palabras de aliento y motivación, y por acogerme como parte de su familia.

A MIS ABUELOS: Juan Antonio Jerez Tórtola, Zoila Esperanza Ortiz Arévalo, Julio Juárez Gómez y Berta Alicia Sánchez Aldana, por su cariño incomparable, por sus consejos y por ser un ejemplo de esfuerzo y dedicación.

A MIS TIOS: Por las palabras de ánimo para seguir adelante y su apoyo en cada etapa de mi vida.

A MIS PRIMOS: Por ser mis amigos y demostrarme cariño, por los buenos momentos que hemos compartido a lo largo de la vida.

A MIS AMIGOS: Por tantos buenos momentos vividos, por las metas que juntos alcanzamos y principalmente por su valiosa amistad.

A MI ASESORA: Miriam Yolanda Najarro López, por brindarme su tiempo y consejo para la realización de mi tesis y ser un ejemplo de profesional del derecho.

A: La tricentenaria Universidad de San Carlos de Guatemala, por ser mi *alma mater*.

A: La Facultad de Ciencias Jurídicas y Sociales, por los conocimientos de superación que adquirí.

PRESENTACIÓN

El trabajo de investigación aplicará el método de investigación inductivo pues se busca analizar el fenómeno que se da en la actualidad con respecto a la identidad personal, así mismo se aplicara el método de investigación cualitativa investigando el aspecto de cualidad al ver la existencia de las personas afectadas y encontrar que ellas se vean beneficiadas en la creación de normas penales, y la evaluación del impacto en las personas que utilizan medios informáticos.

La rama cognoscitiva de la ciencia del derecho a la que pertenece la investigación es la penal y la informática. Es penal, pues busca la creación de un delito dentro del Código Penal de la República de Guatemala, como lo es el delito de Usurpación de identidad personal por medios informáticos, y busca que por cometer el delito el sujeto activo tenga una sanción por medio de una pena. Es informática, pues es un conjunto de normas jurídicas que regulan la aplicación y uso de ordenadores y dispositivos electrónicos cuya actividad está limitada a la afectación que pueda tener dentro de la sociedad.

El contexto diacrónico de la presente investigación es el territorio de Guatemala, al buscar las razones por las que se debe crear en el Código Penal de la República de Guatemala la norma que regule el delito de usurpación de identidad personal por medios informáticos, y el contexto sincrónico en el cual se va a desarrollar esta investigación es el periodo que se comprende desde el año 2018 al año 2023.

El objeto de estudio es la creación del delito de Usurpación de identidad personal por medios informáticos en el Código Penal de la República de Guatemala, realizando la investigación dentro del período del año 2018 al 2023, pues al ir evolucionando la tecnología a través del tiempo, se han cometido ilícitos, los cuales deben de ser regulados en la ley. El sujeto de estudio son las personas que se ven agraviadas por la realización del delito y los que lo realizan el delito de Usurpación De Identidad Personal Por Medios Informáticos. El aporte académico es que la investigación sirva de base para fomentar la existencia del delito dentro del Código Penal Guatemalteco.

HIPÓTESIS

A partir del año 2018 al año 2023 en Guatemala ha crecido el desarrollo de la informática, siendo un elevado grupo de la población guatemalteca el que utiliza medios informáticos, como lo pueden ser las computadoras y los teléfonos celulares actualmente llamados "teléfonos inteligentes".

Dicha evolución está causando como efecto que se produzca una figura jurídica que es la usurpación de identidad personal, esto quiere decir que una persona se apropie de la identidad de otra al utilizar uno de los medios anteriormente mencionados.

La figura de la Usurpación de Identidad Personal por Medios Informáticos consiste en que una persona lleve a cabo determinadas acciones bajo el nombre y apellidos de otra, lo cual se desarrolla de forma más amplia en las redes sociales, por lo que varios guatemaltecos se han visto afectados al no existir una norma en el Código Penal de la República de Guatemala que sancione a los que cometen este delito.

Por este motivo la creación de una norma que penalice a quien cometa el delito de usurpación de identidad por medios informáticos es importante, puesto que es deber del Estado la seguridad y la protección de sus habitantes.

COMPROBACIÓN DE LA HIPÓTESIS

Para comprobar la hipótesis se utilizó el método inductivo, debido a que se razona la importancia de la creación de una ley penal partiendo de observar la falta de regulación dentro de la misma para el delito de usurpación de identidad personal por medios informáticos, así mismo se utiliza el método cualitativo y dentro del mismo se da una comprobación de variaciones concomitantes, pues si varían las circunstancias del actuar, estas circunstancias son las que causan el fenómeno, en este caso el ilícito. Este se da en la creación de la existencia del actuar ilícito de las personas al usurpar la identidad de otra persona y usarla como propia por medios informáticos a través del internet, esto sin el consentimiento del propietario de la identidad, por lo cual si es actuar del actor es diferente, puede estar encasillada en otro delito.

La hipótesis es validada, pues existe el actuar para perjudicar a otra persona, el cual es de usurpar su identidad por medios informáticos, por lo cual se debe de crear la figura penal de la Usurpación de identidad por medios informáticos, estableciendo una pena para el actor del ilícito, otorgándole protección a las demás personas, protegiendo así el bien común.

Existe el problema de que una persona perjudica a otra al usurpar su identidad usando como mascara un medio electrónico, como lo es la computadora y el teléfono celular, por tal motivo que en la actualidad es una actuación recurrente que las personas que utilizan dichos medios se vean vulnerados al no existir sanción para los sujetos activos del delito, ahí nace la importancia que se norme dentro del Código Penal de la República de Guatemala la usurpación de identidad personal por medios informático, al normar este delito se da como beneficio que las personas que cometen este delito puedan ser debidamente sancionadas y así simultáneamente otorgarles protección a todos los guatemaltecos que utilicen medios electrónicos.

ÍNDICE

Pág.

CAPÍTULO II

Pág.

CAPÍTULO III

Pág.

CAPÍTULO IV

Pág.

CAPÍTULO V

CAPÍTULO VI

INTRODUCCIÓN

El vacío legal existente en la legislación penal guatemalteca y el crecimiento del desarrollo de la informática a nivel nacional, siendo un elevado grupo de la población el que utiliza medios informáticos, como pueden ser las computadoras, tabletas, y los teléfonos celulares actualmente llamados "teléfonos inteligentes", por tal motivo está causando el efecto de que se produzca la figura jurídica que es la usurpación de identidad personal por medios informáticos, esto es de relevancia en la actualidad nacional pues esto quiere decir que una persona se puede apropiar de la identidad de otra al utilizar uno de los medios anteriormente mencionados sin tener ninguna consecuencia penal. Pues la usurpación de identidad personal por medios informáticos consiste en que una persona lleve a cabo determinadas acciones bajo el nombre y apellidos de otra, pretendiendo ser ella para causarle daño, y esto lo desarrolla a través del internet y de forma más amplia y popular en las redes sociales, pues de esta forma no tiene un contacto físico, solamente pretende protegerse detrás de una computadora o teléfono celular para no evidenciar que no es ella, por lo que varios guatemaltecos se han visto afectados al no existir una norma en el Código Penal de la República de Guatemala que regule este delito y sancione a los que lo cometen.

El objetivo general fue promover la creación de una norma jurídica dentro del Código Penal de la República de Guatemala, que regule el delito de usurpación de identidad personal cometida por medios informáticos a través del internet.

El desarrollo capitular se realizó de la siguiente manera: En el primero, se abarcó los delitos informáticos los cuales se comenten cuando una persona actúa ilícitamente por medio de dispositivos electrónicos; en el segundo se desarrolló la usurpación de identidad personal por medios informáticos debido al riesgo que se sufre al utilizar la tecnología en la actualidad; en el tercero se observó a los sujetos penales, el sujeto activo del delito siendo quien causa perjuicio contra el sujeto pasivo; en el cuarto se analizó el actuar de los bancos para asegurar las transacciones de sus cuentahabientes; en el quinto se tomó en cuenta el actuar de otros países para proteger a sus habitantes de los ilícitos penales

informáticos; en el sexto se examinó que sancionar la usurpación de identidad personal por medios informáticos va a generar protección jurídica a los guatemaltecos.

Entre los métodos y técnicas desarrollados en la investigación está el método inductivo que busca analizar el fenómeno que se da en la actualidad con respecto a la identidad personal, así mismo se desarrolla un método de investigación cualitativa investigando el aspecto de cualidad al ver la existencia de las personas afectadas y encontrar que ellas se vean beneficiadas en la creación de normas penales, y la evaluación del impacto en las personas que utilizan medios informáticos, y finalmente poder realizar conclusiones generales con fundamento en la indagación de distintos temas que están inmersos en la investigación.

Por lo tanto, la población de la Republica de Guatemala, debe darse cuenta de que la usurpación de identidad personal por medios informáticos es un problema existente y por lo tanto debe de ser normado y creado como una figura ilícita penal.

CAPÍTULO I

1. Delitos informáticos

Los delitos informáticos son las acciones típicas, antijurídicas, culpables y punibles la cual se realiza en el entorno digital, espacio digital o de internet.

1.1 Antecedentes

El desarrollo de la informática tuvo su crecimiento en un corto tiempo, llegando a modificar la forma en como las personas se desarrollaban tanto de forma laboral, social y personal, con ese crecimiento tan repentino, empezaron a surgir algunos problemas que afectaban a las personas.

"Los problemas que la informática tiene con la ciencia del derecho son innumerables, pero tienen un origen común, se le ha olvidado a algunos estudiosos del derecho que el surgimiento de la computadora provoca tantos cambios, como en su momento los monjes escribanos actuaron ante el aparecimiento de la imprenta."[1]

Por lo tanto, en cada momento de la historia se ha ido evolucionando como se causan problemas y el castigo que se implementa al problema causado, por tal motivo el derecho tiene que estar actualizado pues debe otorgar la solución a una problemática y como resultado dar la protección de las personas, por tal motivo, ahora con la aparición de la informática el derecho debe normar de forma legal las actuaciones que perjudican a los habitantes del país que se comenten por esta vía.

El derecho penal "Representa el poder punitivo del Estado y surge como necesidad de ordenar y organizar la vida comunitaria."[2] Por consiguiente, se da el nacimiento del derecho penal como una necesidad de la sociedad para poder llevar en las comunidades

[1] Barrios Osorio, Omar Ricardo. **Derecho e informática.** Pág. 86.
[2] López Guardiola, Samantha Gabriela. **Derecho penal I.** Pág. 12.

una vida pacifica, teniendo como objetivo el castigo de quien no sigue las reglas de convivencia.

Juntamente con el derecho penal nace lo que se conoce como delito, se define que "es la conducta del ser humano que vulnera, cambia o modifica la realidad objetiva, lo cual trae aparejada como una de sus consecuencias, la transformación de la realidad en una sociedad determinada, y otras de ellas son las consecuencias jurídicas, mismas que pueden ser pena privativa de libertad, el pago de una multa y reparación del daño en caso de que así haya sido contemplado por el legislador"[3]. Por lo anteriormente definido se debe comprender que el delito es la acción u omisión que una persona realiza de un acto que no es permitido, dejando como consecuencia un daño a otra persona y también la sanción por haber causado dicho daño, se debe de tomar en cuenta que en para que exista una sanción por un delito, este debe ser tipificado en una ley de carácter penal, púes el derecho penal tiene como principio la exclusión de la analogía, según el Código Penal Guatemalteco, Decreto 17-73, "Por analogía, los jueces no podrán crear figuras delictivas ni aplicar sanciones", siendo así que el delito debe estar de forma específica, pues no se puede utilizar la analogía en el derecho penal.

El derecho informático "resulta como una nueva rama del estudio jurídico, que por el dinamismo del mismo, se encuentra en constante desarrollo, teniendo muy pocos antecedentes a nivel histórico, por su recién aparecimiento, pero se puede mencionar que es a partir del año 1949 con el pronunciamiento de Norbert Wiener (considerado el padre de la cibernética) en su obra cibernética y sociedad, consagra la importancia del derecho y de las comunicaciones expresando la influencia que ejerce la cibernética en uno de los fenómenos sociales más significativos como lo es el jurídico"[4].

Por tal motivo la similitud entre la informática y el derecho es su constante cambio a través del tiempo pues ambos están avanzando, por lo que si la informática avanza el derecho

---

[3] **Ibíd**. Pág.57.

[4] Martínez Chacón Karla Cristina. **Tesis: necesidad de regular jurídicamente el bien informacional.** Pág. 6.

no puede dejar de evolucionar pues deja de normar actuaciones que son de interés tanto nacional como internacional.

Con el crecimiento de la informática nacen los delitos informáticos, con motivo de sancionar a las personas que perjudiquen a otras por medio de la cibernética. "Los delitos informáticos se manifiestan en todas las esferas sociales a nivel nacional e internacional, pueden vulnerar bienes jurídicos tutelados de toda clase principalmente la intimidad y el patrimonio de las personas tanto individuales como jurídicas."[5]

Dado este razonamiento, los problemas informáticos deben ser clasificados como delitos informáticos, los cuales como el autor lo menciona comúnmente se dan en la sociedad sobre bienes jurídicos tutelados, los cuales causan un perjuicio a las personas.

1.2 Definiciones

Es pertinente conocer las definiciones basadas y relacionadas con los delitos informáticos.

1.2.1 Informática

"Es el conjunto de conocimientos que permiten el tratamiento automático de la información y se utiliza para abarcar a todo lo relacionado con el manejo de datos mediante equipos de procesamiento automático como las computadoras."[6] Dada la definición se puede razonar que la informática se utiliza por medio de aparatos en los que se carga la información.

1.2.2 Informática jurídica

"La Informática Jurídica es la aplicación y uso de todo tipo de ordenares y dispositivos electrónicos que permitan el procesamiento de la información en forma automática para

---

[5] Zamora Alvizures José Carlos. **Implementación de la informática forense en la obtención de evidencia digital para combatir los delitos informáticos en Guatemala.** Pág. 99.
[6] Villazán Olivarez Francisco José. **Manual de informática I.** Pág. 8.

la aplicación del derecho"[7] esta definición nos indica que la informática jurídica debe tener un alto conocimiento de informática, tanto técnico, como los entendidos en la materia para que el profesional del derecho pueda aplicarla, pues no basta con que solo posea un conocimiento básico.

1.2.3 Derecho informático

"El derecho informático es el conjunto de normas jurídicas que regulan la aplicación y uso de ordenadores y dispositivos electrónicos cuya actividad está limitada a la afectación que pueda tener dentro de la sociedad."[8] Por lo que en el derecho informático el profesional del derecho solo debe tener conocimientos básicos para poder aplicarlo, pues debe resaltar el derecho en el mismo.

1.2.4 Delitos informáticos

"El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho."[9]

En consecuencia, es necesario encuadrar de manera jurídica los delitos que se cometen pero que su vía de comisión es una computadora y teléfono celular y que por esto no se puede aplicar el delito como tal, sino que se debe crear otra figura delictiva.

1.2.5 Medios informáticos o dispositivos electrónicos

Estos son los resultados que han tenido tanto la ciencia, como la tecnología, lo que ha permitido desarrollar lo que se conoce como nuevas tecnologías de información y

---

[7] Hernández Fuentes Jonathan Efraín. **Informática y derecho.** Pág. 19.
[8] **Ibíd.**
[9] **Ibíd.** Pág. 23.

comunicación, dentro de esa clasificación se encuentra la computadora u ordenador, como la principal de esta clasificación.

1.2.6 Hacker

Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

A estas personas se les puede dar también el nombre de piratas informáticos.

1.2.7 Pishing

Método utilizado por delincuentes para estafar y obtener información confidencial de manera fraudulenta, realizando el ilícito a través de la informática.

1.2.8 Identidad personal

Como su nombre lo indica la identidad personal son las características que una persona posee para que se distinga de los demás, entre estas características podemos encontrar el o los nombres, el o los apellidos, los rasgos físicos, las características y la forma de actuar de una persona, las cuales la hacen diferente.

1.2.9 Usurpación

La usurpación es el apoderamiento de forma ilícita de una propiedad o de un derecho que no le corresponde, esta puede realizarse por la fuerza, con violencia o a través de intimidación, el acto de usurpar tiene un vínculo con la acción de ocupar, cuya voluntad es tener el dominio de alguna cosa.

1.2.10 Usurpación de identidad personal

La usurpación de identidad personal es cuando de forma ilícita una persona se apodera de las características de otra, asiéndose pasar por ella para perjudicarla.

El Código Penal de la República de Guatemala, en su apartado De los Delitos de Falsedad Personal, Artículo 338, Uso ilegitimo de documento de identidad.

"Quien usare como propio, pasaporte o documento legítimo de identidad ajena, será sancionado con prisión de uno a tres años."

Este artículo brinda la protección para que no se usurpe la identidad de una persona, pero es limitado al solo establecer que se da la protección únicamente al usar un documento personal o pasaporte.

1.2.11 Usurpación de identidad personal por medios informáticos

La usurpación de identidad personal por medios informáticos se da cuando una persona pretende apropiarse de la identidad de alguien más o se hace pasar por otra persona al utilizar como medio para su realización una computadora, teléfono celular inteligente, tableta o cualquier otro dispositivo electrónico para entrar de forma ilícita y con objeto de perjudicarla a una página electrónica en donde este tenga su cuenta de correo electrónico, su cuenta en línea de un banco, sus redes sociales, etc.

1.3 Marco legal internacional de los delitos informáticos

Con el avance de la tecnología en el mundo, surge la importancia de que la misma se deba regular, a este aspecto algunas organizaciones internacionales han hecho pública su postura de no reglamentar la misma, si no dar a los países la libertad para normarla para que sea de forma directa, sin embargo, otras han promovido instrumentos jurídicos como lo son:

1.3.1 La Organización de las Naciones Unidas

Quien ha realizado un listado de delitos informáticos, esto con el objeto de que los países estén alerta, así como para que los regulen dentro de su normativa penal, con motivo que se proteja a los habitantes, según el Décimo Congreso de las Naciones Unidas sobre

Prevención del Delito y Tratamiento del Delincuente, que se celebró en Viena (Austria) del 10 al 17 de abril de 2000, son:

- "Espionaje industrial: Los piratas pueden realizar tareas de espionaje avanzado para las empresas o para su propio provecho copiando secretos comerciales que abarcan desde información sobre técnicas o productos hasta información sobre estrategias de comercialización.
- Sabotaje de sistemas: Los ataques como el «bombardeo electrónico» consisten en el envío de mensajes repetidos a una dirección o a un sitio electrónico, impidiendo así que los usuarios legítimos tengan acceso a ellos. El flujo de correspondencia puede hacer rebosar el cupo de la cuenta personal del que la recibe y paralizar sistemas enteros. Aunque ésta sea una práctica extremadamente disruptiva, no es necesariamente ilegal.
- Sabotaje y vandalismo de datos: Los intrusos pueden acceder a sitios electrónicos o bases de datos y borrarlos o cambiarlos, corrompiendo los datos mismos y causando perjuicios aún mayores si se usan datos incorrectos posteriormente para otros fines.
- «Pesca» u «olfateo» de claves secretas: Los delincuentes suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Los «sabuesos» utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.
- Estratagemas: Los estafadores utilizan diversas técnicas para ocultar computadoras que se «parecen» electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos. El famoso pirata Kevin Mitnick se valió de estratagemas en 1996 para introducirse en la computadora de la casa de Tsutomo Shimamura, experto en seguridad, y distribuir en la Internet valiosos útiles secretos de seguridad.
- Pornografía infantil: La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. Durante los pasados cinco años, el número de

condenas por transmisión o posesión de pornografía infantil ha aumentado de 100 a 400 al año en un país norteamericano. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material «ofensivo» que se transmita o archive.

- Juegos de azar: El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la Red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.
- Fraude: Ya se han hecho ofertas fraudulentas al consumidor tales como la cotización de acciones, bonos y valores o la venta de equipos de computadora en regiones donde existe el comercio electrónico.
- Blanqueo de dinero: Se espera que el comercio electrónico sea el nuevo lugar de transferencia electrónica de mercancías o dinero para lavar las ganancias que deja el delito, sobre todo si se pueden ocultar transacciones."

1.3.2 Convenio sobre la Ciberdelincuencia

Que fue firmado en Budapest, Hungría, el 23 de noviembre de 2001, por los países que integran la Unión Europea y Estados participantes, en la que trata con carácter prioritario una postura penal contra la ciberdelincuencia, este convenio es el único que se encarga de la seguridad de la información y trata los delitos contra la Confidencialidad, Integridad y Disponibilidad de los datos y los sistemas informáticos.

Debido a la importancia y al impacto que este convenio ha tenido, algunos países que no forman parte de la unión europea han solicitado unirse ratificando el convenio.

En el cual sus principales objetivos según Convenio de Budapest, 2001, Convenio sobre la ciberdelincuencia son:

- "Aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

- La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones, conectados al área de los delitos informáticos".

Dentro de su contenido norma los siguientes delitos:

- Acceso ilícito.
- Interceptación ilícita.
- Ataque a la integridad de datos.
- Ataques a la integridad del sistema.
- Abuso de los dispositivos.
- Falsificación informática.
- Fraude informático.
- Los delitos relacionados con la pornografía infantil.
- Los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

1.4 Marco legal en Guatemala sobre los delitos informáticos

El Código Penal de la República de Guatemala, Decreto número 17-73, dentro de su contenido norma algunos delitos informáticos, entre los cuales se encuentran.

1.4.1. De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos

Artículo 274 "A". Destrucción de registros Informáticos.

Será sancionado con prisión de seis meses a cuatro años y multa de dos mil a diez mil Quetzales, quien destruya, borre o de cualquier modo inutilice, altere o dañe registros informáticos.

Si la acción contemplada en el párrafo anterior estuviere destinada a obstaculizar una investigación o procesamiento de carácter penal, el responsable será sancionado conforme el Artículo 458 Bis del presente Código.

Artículo 274 "B". Alteración de programas.

La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras.

Artículo 274 "C". Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

Artículo 274 "D". Registros prohibidos.

Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Artículo 274 "E". Manipulación de información.

Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.

Artículo 274 "F". Uso de información.

Se impondrá prisión de seis meses a dos años, y multa de dos mil a diez mil quetzales al que sin autorización, utilice u obtenga para sí o para otro, datos contenidos en registros informáticos, bancos de datos o archivos electrónicos.

Artículo 274 "G". Programas destructivos.

Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o instrucciones

destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

Artículo 275 Bis. Alteración fraudulenta.

Toda persona individual o jurídica que comercialice los terminales móviles que hayan sido reportados como robados o hurtados y que aparezcan en la BDTR (lista negra) establecida por cada operador, así como toda persona que reprograme o en cualquier forma modifique, altere o reproduzca en dichos terminales móviles, el numero serial electrónico (ESN) del equipo terminal móvil, el Numero de Identidad de Equipo Móvil (IMEI). Para el Sistema Global para Comunicaciones Móviles (GSM), o cualquier otra característica de identificación propia de los terminales móviles, o reprograme, altere o reproduzca en forma fraudulenta cualquier Modulo de Identidad del Suscriptor (SIM) para el Sistema Global para Comunicaciones Móviles (GMS), será responsable del delito de alteración fraudulenta, el cual será sancionado con pena privativa de libertad de cuatro a seis años, y multa de veinticinco mil quetzales a cincuenta mil quetzales.

1.4.2 De los delitos de falsedad personal

Artículo 335. Usurpación de funciones.

Quien sin título o causa legítima, ejerciere actos propios de una autoridad o funcionario, atribuyéndose carácter oficial, será sancionado con prisión de uno a tres años.

Artículo 336. Usurpación de calidad.

Quien se arrogare título académico o ejerciere actos que competen a profesionales, sin tener título o habilitación especial, será sancionado con prisión de cinco a ocho años, y multa de cincuenta mil a doscientos mil quetzales.

Si del resultado del ilegal ejercicio se derivare perjuicio a tercero, la sanción señalada en el párrafo que antecede, se elevará en una tercera parte.

Artículo 337. Uso público de nombre supuesto.

Quien usare públicamente nombre supuesto, será sancionado con multa de 500 a 3000 quetzales.
Si el uso del nombre supuesto tuviere por objeto ocultar algún delito, eludir una condena, o causar algún perjuicio al estado o a un particular, además de la sanción señalada en el párrafo que antecede, se impondrá al responsable prisión de uno a dos años.

Artículo 338. Uso ilegitimo de documento de identidad.

Quien usare como propio, pasaporte o documento legítimo de identidad ajena, será sancionado con prisión de uno a tres años. Igual sanción se aplicara a quien cediere a otro, para que lo utilice su propio pasaporte o documento legítimo de identidad.

La sanción se incrementará a la mitad, cuando el uso ilegitimo del documento de identidad sea para fines electorales.

Si el delito es cometido por funcionario o empleado del tribunal supremo electoral, integrante de junta electoral departamental, junta electoral municipal, junta receptora de votos, funcionario o empleado del estado de cualquiera de sus organismos o instituciones autónomas, descentralizadas y no gubernamentales, independientemente de su forma de elección o tipo de vínculo legal laboral, se le aplicara además de la pena, la inhabilitación para el ejercicio de empleo o cargo público que desempeñe.

CAPÍTULO II

2. Usurpación de identidad personal por medios informáticos

Se lleva a cabo cuando una persona realiza determinadas acciones bajo el nombre y apellidos de otra, pretendiendo ser ella para causarle daño, y esto lo desarrolla a través del internet y de forma más amplia y popular en las redes sociales.

2.1 Elementos de la usurpación de identidad personal por medios informáticos

Estos elementos son los cuales le dan forma a la usurpación de identidad personal por medios informáticos como un delito, así como evidencian la importancia que tiene el añadirla al ordenamiento jurídico penal guatemalteco, los cuales constan en una serie de conductas ilícitas que las personas pueden hacer, teniendo estos interés e incidencia en la calificación penal. Los elementos son: La apropiación de información personal por medios informáticos, la transferencia o cesión de datos personales, y la utilización o facultad arrogada de manera indebida para su utilización sobre dichos datos personales.

2.1.1 La apropiación de información personal por medios informáticos

"las conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa."[10]

El cual supone que es la realización de una actividad por medios convencionales o informáticos, el cual contiene un carácter externo en el sujeto activo del delito, el cual busca apoderarse de forma indebida e ilícita de datos personales que no le pertenecen en soportes lógicos o materiales. Según este orden de ideas, se puede analizar como primer punto, la existencia de elementos intangibles que se dan en el apoderamiento de soportes lógicos, aun cuando estos pueden tener un soporte material, puesto que, en la actualidad en la mayoría, las bases de datos se encuentran automatizadas, teniendo un

[10] Romero Flores Rodolfo. **Las conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa** Pág. 852.

carácter incorpóreo, dando como resultado la operación fraudulenta de usurpación de bienes incorpóreos o bien llamado datos automatizados.

2.1.2 La transferencia o cesión de los datos personales

Este elemento implica una relación de causalidad con el primer elemento, pues al momento de que el sujeto activo sea propio de datos personales en soportes lógicos o materiales, y su intención es transferir o ceder los datos que obtenga mediante una retribución o compensación económica la cual también tiene carácter de indebida.

Al obtenerse datos personales de forma ilícita, estos pueden acabar en manos de tercero y en gran cantidad de veces hasta en grupos de delincuencia organizada, mismos que su objetivo es la realización de acciones ilegales, es el caso que al realizarse las bases de datos de forma automatizada ya sea de personas físicas o colectivas, se corre el peligro de que estas puedan ser comercializadas sin conocimiento, ni autorización de los sujetos pasivos.

2.1.3 La utilización o facultad arrogada de manera indebida para su utilización sobre dichos datos personales

Este elemento desarrolla las calidades atributivas y relacionales con el ente de imputación jurídica, son derivadas a un nuevo ente para producir actos o consecuencias legales para ser atribuidas al ente jurídico original sobre del cual se obtuvieron datos personales.

2.2 Riesgos que se derivan del extravío, robo o hurto de un dispositivo electrónico

Un dispositivo electrónico es un aparato que tiene capacidades de procesamiento, a su vez este puede tener una conexión de manera permanente o intermitente a internet, y en el que se pueden llevar a cabo una sola o variadas tareas.

Entre los dispositivos electrónicos más destacados se pueden mencionar: la computadora personal, la laptop, la Tablet, y el teléfono móvil. En estos 4 tipos de

dispositivos se pueden tener las funciones de ingresar a internet, almacenamiento de fotografías, videos, números telefónicos, documentos, y aplicaciones que la persona desea tener.

Con el uso de la conexión a internet y con la ayuda de las diversas aplicaciones una persona puede comunicarse de manera inmediata con otra, sin importar la distancia en la que se encuentren, redactar documentos, hacer publicaciones en tiempo real de imágenes, videos, frases.

2.2.1 Riesgos que se derivan de extravío, robo o hurto de los dispositivos electrónicos

- En estos dispositivos las personas guardan fotografías y videos propios, de familiares, sociales y de sus gustos, el riesgo está en que la persona que encuentre o que haya cometido el ilícito del hurto o robo, puede tener acceso a ver y a tener estas imágenes y videos, y así utilizarlas o tener la información sobre cómo es la persona, su familia, sus amistades, gustos y muchas veces hasta sus bienes.

- En estos dispositivos las personas tienen guardado los números telefónicos de sus familiares y de su círculo social, por lo que el riesgo está en que la persona que lo encuentre o que haya cometido el delito del robo o el hurto puede tener acceso a estos.

- Las personas mantienen abiertas en sus dispositivos electrónicos sus cuentas de correos electrónicos y sus redes sociales, el riesgo está en que el que encuentre su dispositivo electrónico o el que robo o hurto su dispositivo puede tener acceso a ellas, por lo cual tienen acceso a gran cantidad de información de la persona (nombre completo, edad, sexo, estado civil, fotografías, amistades, lugares que frecuenta, profesión u oficio, lugar en el que labora, gustos propios, etc.) pudiendo de esta forma utilizarlas a su conveniencia y así usurpar esta información.

- A estos dispositivos las personas le tienen mucha confianza por tener su acceso inmediato, por consiguiente, guardan usuarios y contraseñas de correos electrónicos, redes sociales, cuentas en línea de bancos, en consecuencia, está que la persona que encuentra el dispositivo o el que cometió el ilícito penal puede tener acceso a ellas y manejarlas a su conveniencia.
- En algunos casos no afecta únicamente a la privacidad personal del dueño del celular extraviado, sino que puede ocasionar una brecha en la seguridad corporativa de la empresa en donde labora la persona que extravío, fue robada o hurtada de su dispositivo electrónico.

Se debe tomar en cuenta estos riesgos que se pueden dar al extraviar, ser hurtados o robados los dispositivos electrónicos.

Para ello se puede desarrollar un listado explicando el cómo se puede prevenir que esto suceda, para así evitar arriesgar su información personal.

Pues se busca evitar que la información personal de cada persona caiga en manos de alguien que le pueda dar un uso negativo a la misma.

2.2.2 Formas de prevenir el extravío robo o hurto de dispositivos electrónicos

- Evitar el uso de los dispositivos electrónicos en lugares que se sabe o se vea que no es un sito seguro para hacerlo.

- Por ningún motivo dejar su equipo a la vista en sitios públicos si no se está utilizando. Estos sitios son donde ocurren la mayoría de los casos de extravío y robo de un dispositivo electrónico.

- En casos de dispositivos móviles como el celular, se aconseja que no se contesten mensajes o llamadas en cualquier lugar, esto se debe a que cuando uno contesta llamadas o mensajes se presta menos atención a su entorno.

- En caso de dispositivos móviles como el celular, las personas están acostumbradas a llevar su dispositivo en la mano o de sacarlo en lugares públicos o con gran afluencia de personas, por ese motivo se aconseja que se guarde en un lugar seguro, ya que al llevarlo a la vista aumenta el riesgo a que se lo quiten sin importar en lugar en el que se encuentre.

2.2.3 ¿Qué hacer en caso de que se realice el extravío, hurto o robo de un dispositivo electrónico?

1. En caso del teléfono celular comunicarse con la empresa de telefonía móvil que se haya contratado para solicitar el bloqueo de este inmediatamente y así ya no lo puede utilizar el que lo ha encontrado, robado o hurtado.

2. Interponer una denuncia en la Policía Nacional Civil o el Ministerio Público como requisito de reposición o trámite para recuperar el número de celular y adquirir otro dispositivo.

3. La denuncia será presentada a la compañía telefónica que ratificará el bloqueo.

4. Cerrar cuentas abiertas en este dispositivo.

2.3 Seguridad de los dispositivos electrónicos

En consecuencia, del avance de la tecnología, se deben desarrollar sistemas de seguridad en los cuales las personas puedan proteger la información que ingresen o almacenen en sus medios informáticos o en sus dispositivos electrónicos, con el objetivo de proteger la información privada.

2.3.1 Algunas formas de seguridad son

- Bloquear la pantalla con una contraseña difícil.

- Mantener el teléfono cerrado o bloqueado si no está en uso; no descuidarlo ni perderlo de vista.

- Evitar guardar información confidencial en el dispositivo móvil.

- Realizar periódicamente un respaldo físico o en la nube con la información más valiosa.
- Utilizar programas de seguridad en el dispositivo móvil que ayuden a localizarlo si es extraviado o robado.

- Guardar por separado datos como número telefónico, el modelo, la contraseña para desbloquear, así como el número de IMEI.

- Guardar la factura de compra como el comprobante imprescindible para presentar la correspondiente denuncia en caso de pérdida o robo.

- Anotar todos los datos del equipo portátil o dispositivo móvil, incluyendo número de serie y dirección MAC, un dato de red que identifica de forma única el equipo.

- Hacer una marca discreta en su equipo y guardar una fotografía de esta para demostrar inequívocamente que es de su propiedad. También se puede incluir una pegatina con su nombre y teléfono móvil. No todas las pérdidas de equipos móviles son por robo y en caso de extravío podrán ponerse en contacto el que ha extraviado su dispositivo.

- Asegurase de realizar copias de seguridad de todos sus datos en caso de viajes o si es un usuario de negocio móvil. Si el extravío se produce al menos se puede recuperar los datos. Así mismo, mantener sus archivos más valiosos en carpetas cifradas y, si utilizas servicios de almacenamiento on-line, guarda las contraseñas a buen recaudo.

- Utilizar sistemas avanzados de protección de datos como la cartera Client Security de HP, que incluye HP Drive Encryption, HP Device Access Manager con Just in Time Authentication y HP Secure Erase.

- Activar los sistemas de seguridad integrados del equipo, como una contraseña de desbloqueo la cual se recomienda que sea extensa con uso de mayúsculas, números, el lector de huella digitales o el reconocimiento facial.
- Bloquear el acceso al BIOS y a la cuenta de administrador con una contraseña lo más fuerte posible.

- Utilizar los sistemas de anclaje para asegurar el equipo, especialmente en seminarios, conferencias, bibliotecas o zonas públicas de transporte.

- Valorar la contratación de un seguro específico para el caso de robo o extravío. Un seguro estándar no suele incluir el robo en las coberturas.

- Activar sistemas antirrobo específicos como el Intel Anti-Theft que evita el arranque del equipo a nivel de hardware (CPU/Chipset/BIOS/Drivers) y también el acceso a los datos de la unidad de almacenamiento.

- Alternativamente, se puede utilizar de servicios de seguridad multiplataforma como Prey para intentar recuperar computadoras, tablets o smartphones perdidos o robados rastreando su ubicación.
  Es gratuito para uso básico (hasta tres equipos) e incluye una gran cantidad de opciones en las versiones de pago.

- Encuentra tu dispositivo con Windows 10 utilizando esta característica que Microsoft ha implementado para su último sistema operativo. Encuentra Mi Dispositivo, es una función que hace tiempo estaba implementada en Windows Phone para localización de smartphones y ahora está disponible para ordenadores personales facilitando la tarea de localizar equipos informáticos perdidos o robados. Su activación se realiza

de forma sencilla usando una cuenta Microsoft ID desde la herramienta de Configuración del sistema, apartado Actualización y Seguridad.

- Evitar acceder a la conexión WIFI en lugares que puedan ser inseguros.

2.4 Mecanismos utilizados para la usurpación de identidad personal por medios informáticos

Existen diferentes mecanismos que las personas con conocimiento de informática pueden llevar a cabo para cometer el acto ilícito de usurpar la identidad de otros, así apropiándose de su información y rasgos que lo caracterizan por medios informáticos o aparatos electrónicos, entre estos métodos se pueden mencionar los siguientes:

2.4.1 Ingeniería social

Es una técnica utilizada para obtener información a través de la interacción social, la manipulación y el engaño, y ocurre, típicamente, en conversaciones directas entre el que pretende hacer el ilícito y la víctima. El sujeto activo consigue que su víctima no se dé cuenta cómo ni cuándo dio todos los datos necesarios para la usurpación de su identidad.

En esta práctica se recurre a la manipulación de la psicología humana mediante el engaño. El delincuente actúa a partir de la premisa de que, en la cadena de seguridad de la información, el ser humano es el eslabón más débil debido a que la víctima es la que otorga su información.

Como ejemplo de la forma en la cual se puede dar la usurpación personal por medios informáticos utilizando la ingeniería social es en una simple conversación por medio de la cual una persona conoce a la otra, es ahí la importancia que tiene el no dar la información personal a una persona que no sea confiable, de la información en la que se puede llevar a cabo la ingeniería social pueden ser: el nombre completo, edad, estado civil, que estudia, cuáles son sus gustos, que hace, en donde labora, en donde vive, etc.

Algunas formas de ataque que incluyen ingeniería social son: el pretexting y la extorsión telefónica.

- **Pretexting:** En esta variación de la ingeniería social, el atacante debe tener un estudio previo de la información de la víctima potencial, para así, crear y utilizar un escenario favorable con el objetivo de persuadir a una víctima y obtener información.

  El atacante puede acoplarse a una víctima específica de manera que aumenta la posibilidad de conseguir información o que la víctima realice acciones específicas a su voluntad.

  Un ejemplo de esta modalidad de ingeniería social es cuando alguien ha observado a otra persona para ver su forma de actuar, y como resultado de su forma de actuar puede saber cómo hacer que ella le de la información que necesita.

- **Extorsión telefónica:** en esta variación de la ingeniería social, el atacante realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, por ejemplo, un técnico de soporte o un empleado de alguna organización con el objetivo de obtener datos de la víctima. Es un modo muy efectivo y lo único que se requiere es un teléfono.

2.4.2 Observación

La observación es una técnica muy antigua que se centra en poner atención a las acciones que realiza la víctima y que son de interés para el atacante.

El atacante debe guardar discreción para no ser descubierto, por esta razón, se auxilia utilizando herramientas destinadas al espionaje (por ejemplo, binoculares, aparatos para escuchar a distancia, entre otros).

El objetivo de esta técnica es obtener información preliminar para cometer ataques.

Un ejemplo de esta modalidad de usurpación de identidad personal es cuando una persona silenciosamente se acerca a otra sin llamar la atención para escuchar lo que está hablando esta para así poder sacar información de ella sin tener una relación directa con la víctima.

2.4.3 Shoulder surfing o espionaje por encima del hombro

Técnica derivada de la observación, la particularidad que tiene es que el espionaje a los usuarios se realiza de cerca, para obtener información confidencial.

Sólo basta con permanecer observando sigilosamente por la espalda de la víctima las teclas que digita, el monitor o cualquier otro soporte de información que pueda ser de interés para obtener información. Esta técnica se utiliza comúnmente para obtener contraseñas, números PIN, códigos de seguridad y datos similares.

Un ejemplo de esta forma de usurpación de identidad personal se puede dar cuando una persona va a un lugar en el que se alquilan máquinas computadoras e internet en ellas, y otra persona se coloca atrás de ella de forma silenciosa para ver lo que está escribiendo y así poder ver la forma que utiliza para ingresar y logrando así acceder a sus cuentas.

2.4.4 Eavesdropping o parar la oreja

Esta técnica se trata de explotar el sentido del oído para capturar información privilegiada cuando se está cerca de conversaciones privadas.

Por ejemplo, cuando un administrador de sistemas le comenta a un ejecutivo cuál es la clave que puso en una aplicación crítica.

2.4.5 Dumpster diving

Es una técnica que se centra en buscar información valiosa en la basura. Tirar cualquier tipo de documentos sin un debido proceso de destrucción es una práctica que puede resultar riesgosa, pues se pueden rescatar de la basura datos importantes contenidos en documentos desechados sin ser destruidos previamente.

Por ejemplo, cuando las personas desechan en la basura documentos o información importantes y no la destruyeron correctamente, puede ser que otro la encuentre y se aproveche de esto.

2.4.6 Asalto al buzón de correo

Es un delito centrado en el robo de la correspondencia que se encuentra en los buzones de correo sin seguro, de los cuales se pueden sustraer documentos con información valiosa (estados de cuenta bancarios o de tarjetas de crédito, o cualquier otro documento).

Un ejemplo de esta modalidad es cuando una persona llega a una casa que no es la suya para extraer del buzón de correspondencia un estado de cuenta el cual contiene la información de la víctima.

2.4.7 Sin acceso a internet y con apoyo de alguna herramienta tecnológica

En esta categoría, se recopilan las técnicas utilizadas para usurpar la identidad de una persona las que no requieren tener acceso a un punto de conexión de internet, pero que se refuerzan con la ayuda de algún dispositivo electrónico.

Dentro de estas técnicas hay tres descritas por el INAI, estas son:

- **Skimming o clonación de tarjetas (crédito o débito)**
  Esta técnica consiste en realizar una copia de una tarjeta sin el consentimiento del dueño. Los estafadores utilizan diferentes tipos de dispositivos electrónicos (clonadoras) programados para guardar los datos contenidos en la cinta magnética (número de tarjeta, fecha de vencimiento, código valor de verificación, banco, nombre del titular), para posteriormente reproducir o clonar la tarjeta en un plástico diferente. Este método sólo puede ser utilizado en el momento en que la víctima realiza una transacción con su tarjeta.

  Un ejemplo, cuando una persona llega a un cajero automático al cual le insertaron un dispositivo clonador, esta persona sin saberlo ingresa su tarjeta y su pin, automáticamente este aparato guarda la información de esta tarjeta para poderla clonar.

- **Vishing**

  Es una práctica criminal fraudulenta realizada por teléfono, en la cual a través de ingeniería social se pretende obtener información. El término vishing es una combinación de las palabras voice (voz) y phishing (método de suplantación de identidad). En un intento de vishing, el estafador llama pretendiendo ser miembro de algún corporativo y para informar sobre actividad sospechosa reportada en las cuentas de la víctima. Basándose en esta mentira, envuelve a la víctima para que ésta verifique información por teléfono.

  Ejemplo, una persona recibe la llamada en la cual otra que es la que llama se identifica que es trabajador de un banco (lo cual es falso), y solicita la información inmediata de los datos de su cuenta en línea.

- **SMiShing**

  Consiste en una variante fraudulenta del phishing, donde a través de técnicas de ingeniería social se realizan envíos selectivos de mensajes SMS dirigidos a usuarios de telefonía móvil con el fin de que visiten una página web fraudulenta.

  Mediante reclamos atractivos con alertas urgentes, ofertas interesantes o suculentos premios, tratan de engañar al usuario aprovechando las funcionalidades de navegación web que incorporan los dispositivos móviles actuales.

  Ejemplo, una persona recibe en su teléfono celular un mensaje de texto que indica que un banco del sistema nacional requiere que actualice su información en determinada página electrónica, la cual no es la verdadera del banco.

2.4.8 Con acceso a internet

Existen algunos métodos fraudulentos para obtener de manera fraudulenta los datos de información personal las cuales único sin cinco técnicas descritas por el INAI y lo único que es necesario es que se pueda acceder a internet, es que el usuario haga uso de alguna aplicación, alguna plataforma en internet o acceda a un correo electrónico:

- **Spam**

  Se puede considerar como spam a cualquier mensaje de correo electrónico enviado a varios destinatarios que no solicitaron tal mensaje, también llamado correo electrónico basura; un mensaje de spam debe cumplir con varios aspectos: ser enviado de forma masiva, ser un mensaje no solicitado por el usuario y tener contenido engañoso (habitualmente de tipo publicitario).

  Una vez que el usuario accede al contenido engañoso provisto por el spam, se pueden presentar dos escenarios, el primero, cuando el usuario es direccionado a una página web controlada por el atacante en donde mediante el llenado de formularios proveerá información personal que posteriormente se utilizará para cometer un fraude; el segundo escenario se presenta cuando el usuario descarga el contenido adjunto al spam, lo que se traduce en una invasión a su equipo de cómputo mediante un virus que roba la información del dispositivo.

  Un ejemplo, cuando a una persona le llega a su correo electrónico un correo estableciendo que se ha ganado algo, que solo debe acceder a determinada página, al acceder a la página debe llenar un formulario con toda su información la cual le llega al delincuente para cometer fraude con la información dada.

- **SPim**

  Es un caso específico de spam a través del cual se envían mensajes instantáneos cuyo contenido puede incluir spyware, registradores de pulsaciones, virus, vínculos a sitios de phishing o invitaciones para suscribirse a servicios o promociones falsas mediante el envío de mensajes instantáneos a un servidor controlado por el atacante, cuyo objetivo es tomar el control de la lista de contactos para suplantar la identidad del afectado.

  Un ejemplo, llega al correo electrónico de una persona un correo que indica que debe acceder a una página electrónica y al acceder su computadora se infecta de un virus que va a controlar su lista de contactos.

- **Registradores de pulsaciones**

  Un registrador de pulsaciones es una forma de software espía que guarda las letras que fueron pulsadas en un documento de texto. Cuando un usuario que tiene este software instalado está navegando en la web, visitando sitios de comercio o banca electrónica, el registrador de pulsaciones puede registrar los caracteres digitados. Este software es una combinación cuidadosamente elaborada en formato HTML, en la que entre las hojas de estilo, capas, cuadros de texto y objetos de contenido, un usuario al estar escribiendo, lo hace en un marco invisible controlado por un atacante.

  Ejemplo, una persona con conocimiento de informática descarga en la computadora de otra persona una aplicación llamada registrador de pulsaciones, para así ver todo lo que se escribe en esa computadora y tener su información.

- **Phishing o suplantación de identidad**

  Es una estafa en línea, a través de la utilización de spam, sitios web falsos, mensajes de correo electrónico, mensajes instantáneos, cuya finalidad es obtener de los usuarios de internet información confidencial, tales como contraseñas o información detallada sobre tarjetas de crédito u otra información bancaria. El término proviene de la palabra fishing (pesca) y hace alusión a pescar usuarios para obtener información financiera y sus contraseñas. Los autores del fraude, conocidos como phishers simulan ser empresas legítimas, y pueden utilizar el correo electrónico para solicitar información personal e inducir a los destinatarios a responder a través de sitios web maliciosos.

  Los phishers suelen utilizar tácticas alarmistas o solicitudes urgentes para tentar a los destinatarios a responder. Los sitios de robo de identidad parecen sitios legítimos, ya que tienden a utilizar las imágenes de Copyright de los sitios legítimos; sin embargo, no incluyen el protocolo seguro de transferencia de hipertexto (identificado en las direcciones electrónicas como el https://). Los mensajes fraudulentos generalmente no están personalizados y es posible que compartan propiedades similares, como detalles en el encabezado y en el pie de página.

Ejemplo, una persona crea una página electrónica falsa, copiando exactamente la forma de la original para confundir a la víctima, solo cambiando una letra en el nombre de la página para que no sea notorio, la victima ingresa sus datos y al acceder le envía la información al creador de la página falsa, pudiendo así hacer transacciones a su nombre.

- **Pharming**

  Es una vulneración que tiene la finalidad de redirigir a un usuario de internet que navega en páginas web a una página falsa diseñada para robarle información personal. A diferencia del phishing, el pharming está programado para atacar al equipo de la probable víctima; hace que la navegación web se redireccione a servidores plagados de sitios controlados que tienen un aspecto similar al que el usuario trata de ingresar, es decir, cuando la víctima introduce una dirección electrónica correcta, ésta es enrutada o redireccionada hacia el servidor del atacante. En pocas palabras, el pharming es una granja de víctimas.

CAPÍTULO III

3. Los sujetos del delito informático

Los sujetos del derecho penal son los sujetos activos y los sujetos pasivos, por ser estos los más generalizados en la doctrina penal.

3.1 Sujeto activo del delito informático

"El sujeto activo es el autor del delito, es decir, la persona que ejecuta todo o parte de la conducta ilícita descrita en el tipo"[11].

El sujeto activo es el que lleva a cabo la realización de un delito, ya sea buscando causar un daño físico o moral a determinada persona, o determinado grupo de personas, aunque también puede que, al realizar el delito, el sujeto pasivo no busque causar un daño, sino que sea resultado de una acción que no buscaba cometer el delito.

Existen casos en los que exista más de una persona que realice el delito ya sea una parte de él o que solo haya sido el actor intelectual del delito, en estas situaciones a todos los que han participado de forma activa para la realización del delito se les llama el sujeto activo y tienen el mismo grado de culpabilidad por el delito consumado.

En el caso de la usurpación de identidad personal por medios informáticos solo existe hasta el momento la antijuricidad del actuar, al momento en el cual una persona usurpa la información personal de otra por medios informáticos, está cometiendo una acción que va en contra de la moral, de las leyes y de las buenas costumbres, pero al no estar en la normativa legal y tener una sanción, no se cumple las características necesarias para ser un delito.

Para que una persona se convierta en sujeto activo de un delito, tiene que existir en la normativa vigente, como una acción típica, antijuridica y punible, por lo tanto, debe estar

---

[11] Balmaceda Hoyos Gustavo. **Estudios de derecho penal general.** Pág. 200.

establecido en la ley, tiene que ser un actuar que sea en contra de la ley y las costumbres, y tiene que existir una sanción para el actuar.

Al momento que se norme en el Código Penal guatemalteco la usurpación de identidad personal por medios informáticos, se va a considerar el mismo como un delito, por tal motivo cumpliría con las características del delito, siendo este, típico, antijurídico y punible, hasta ese momento se le va a conocer al infractor como sujeto activo del delito informático.

El sujeto activo "Es la persona física que comete el delito; el sujeto activo es siempre una persona física, independientemente del sexo, la edad, la nacionalidad y otras características"[12].

Esto quiere decir que el que comete un delito siempre va a ser una persona física e individual, pues el ser humano es capaz de tomar decisiones sobre cómo actuar ante diferentes situaciones que se le puedan presentar.

En consecuencia, si comete un delito es su decisión, por este motivo se debe comprender que un animal, un objeto inanimado, ni una persona jurídica puede ser un sujeto activo.

Una persona jurídica no puede ser un sujeto activo debido a que el actuar de la misma siempre va relacionado al actuar de una o varias personas.

El sujeto activo tiene el mismo grado de culpabilidad esto sin importar la edad que tenga, el sexo de sea, o la nacionalidad que sea es la misma, aun cuando la sanción que se le imponga sea diferente, como lo es en el caso de menores de edad.

Por lo tanto, el sujeto activo de un delito informático es la persona individual o el grupo de personas individuales autores de cometer una actividad criminal con el uso de técnicas informáticas, ya sea ejecutándolo totalmente o en parte.

---

[12] Amuchategui Requena Griselda. **Derecho penal.** Pág. 37.

3.2 Sujeto activo del delito informático y su impacto en la sociedad

El progreso de la informática ha sido de mucho beneficio por motivo de que permite que con el uso de un aparato electrónico y conexión a internet una persona pueda comunicarse con otra de forma inmediata, hacer investigaciones, hacer trabajos, estudiar, y más.

El sujeto activo debe de tener conocimiento de informática y desarrollo de la web, así como también de ingeniería social, puesto que deben crear engaños que resulten efectivos para que las personas que se conviertan en sus víctimas puedan resultarles atractivos y así ser dañados sin tener el conocimiento de lo que va a ocurrir y así el sujeto activo puede alcanzar su objetivo el cual es atacar.

Por tal motivo el impacto que se da en la sociedad cuando una persona comete un delito informático son de gran negatividad.

En el periódico guatemalteco, denominado Prensa Libre, el 2 de septiembre de 2018, en la página 17, se da a conocer que Latinoamérica es una región que está siendo fuertemente atacada con delitos informáticos, siendo uno muy sobresaliente la usurpación de identidad. Se realiza un comparativo de usuarios atacados por países en el año 2017 y en el 2018, en el año 2017 los países más afectados por delitos informáticos son: en primer lugar, Brasil, consecutivamente Bolivia, Perú, Venezuela y Ecuador; en el año 2018 los países más afectados por delitos informáticos son: en primer lugar Brasil, consecutivamente Venezuela, Argentina, Perú, Bolivia, Chile, Colombia, El Salvador, Panamá, Costa Rica, Guatemala, Honduras, Nicaragua y Belice.

En el mismo periódico referido se realiza un porcentaje de sitios de phishing bloqueados en Guatemala de enero a agosto de 2018, por categorías: un 50.30 por ciento en Bancos, un 16.07 por ciento en Portales de internet globales, como los motores de búsqueda, un 10.57 por ciento en Sistemas de pago en línea, un 6.68 por ciento en servicios web, un 4.37 por ciento en Sitios de compras en línea, un 3.65 por ciento en redes sociales y un 3.44 en Aerolíneas.

Según los datos detallados anteriormente demuestran que a partir de año 2018 al año 2023 los delitos informáticos han sido crecido en gran escala, siendo Guatemala un país en el que se ha dado estos delitos, siendo uno delito de los más comunes dentro de los delitos informáticos, la usurpación de identidad personal por medios informáticos, por lo tanto, se evidencia que Guatemala es un país en el cual ocurre la usurpación de identidad personal por medios informáticos.

Por lo tanto, también se da a conocer que las formas por las cuales los sujetos activos cometen la usurpación de la identidad personal por medios informáticos son variadas siendo la más frecuentemente utilizada en bancos, desarrollando esta forma por medio de tarjetas de crédito, cajeros automáticos, información confidencial del banco indebidamente destruida.

Luego se encuentra la siguiente forma la que es en portales de internet globales, como los motores de búsqueda, dándose esta forma por medio de buscadores, en los cuales las personas pueden encontrar lo que necesiten, como ejemplo de estas se encuentra Google, Yahoo, YouTube, entre otros.

Seguidamente se encuentra otra forma la que se da en sistemas de pago en línea, esta forma se utiliza ya que brinda mayor comodidad a las personas al poder hacer pagos, depósitos, y créditos en línea, ejemplos de esta se encuentra la banca electrónica de los diferentes bancos, PayPal, Xoom, entre otros.

Posteriormente se da otra forma la que es los servicios web, la misma se desarrolla por medio de páginas electrónicas que ofrecen algún servicio como lo puede ser de información, videos, contenido, ventas, entre otros.

Seguidamente está la forma de servicios de compras en línea, esta se lleva a cabo por medio de páginas web en las cuales ya sea una empresa que brinda los productos, o las que les permiten a las personas vender sus productos, ejemplo de estas esta Amazon, Olx, Cemaco, Siman, entre otras.

Luego se encuentra la forma que es por medio de redes sociales, esta se da cuando en las páginas web les brindan a las personas la posibilidad de estar en contacto con otras personas, saber sus gustos, ver fotografías, brindando en estas sus datos personales, como ejemplo de estas se encuentran Facebook, WhatsApp, Instagram, Twitter, LinkedIn, entre otras.

Por último, se encuentra la forma que es por aerolíneas, esta se desarrolla por el motivo de que las personas pueden comprar sus vuelos en avión en las páginas web de las aerolíneas, así como también pueden hacer el prechequeo en línea, otorgando así datos personales.

Por tal motivo la facilidad que se tiene en la actualidad para utilizar el internet por medio de los dispositivos electrónicos tiene como resultado que una persona se conviertan en el sujeto activo al cometer un delito informático, como lo es la usurpación de identidad personal, pues sienten hasta algún grado una protección, al no hacerlo de manera física o personal y al no tener una sanción si lo realizan.

Dadas las circunstancias, al momento en que se norme en el Código Penal guatemalteco vigente, la usurpación de identidad personal por medios informáticos, imponiéndole una sanción a los sujetos activos que cometan el delito mencionado, los índices de recurrentes del delito bajarían, en lugar de irse incrementando con el tiempo, por tal motivo si no se norma el mencionado delito, seguirá incrementándose a lo largo del tiempo, por ser una forma popular de cometer delitos en la actualidad.

3.3 Sujeto pasivo del delito informático

"Sujeto pasivo es la persona física o moral sobre quien recae el daño o peligro causado por la conducta del delincuente, se le denomina también victima u ofendido"[13].

El sujeto pasivo es en el cual recae el actuar del sujeto activo, para provocarle un daño o un peligro hacia su persona.

---

[13] **Ibíd.** Pág. 38.

Por tal motivo resultado del actuar del sujeto activo, causa que el sujeto pasivo sea el perjudicado en la realización de una acción, la cual frecuentemente, aunque no en todos los casos busca causarle un daño ya sea físico o moral, esto con motivo de afectarlo para que no pueda realizar alguna actividad con tranquilidad.

La doctrina le conoce al sujeto pasivo también con los nombres de víctima u ofendido, pues se busca evidenciar que es sobre el que recae el actuar ilícito, siendo evidentemente el afectado, y al cual la ley le debe la protección jurídica para sancionar al que lo perjudica, y al mismo tiempo que al ver el sujeto activo las consecuencias del actuar ilícitamente, lo proteja también para que no se convierta en victima al estar debidamente establecido en la ley.

"El sujeto pasivo de un delito podrá ser tanto una persona en especial, como también toda la sociedad, el Estado, personas jurídicas, la familia como concepto en sí, etc."[14]

Al ser el sujeto pasivo el perjudicado de la realización de un delito, puede que el delito cometido sea en contra de determinada persona causando el daño a solo un sujeto, así también puede que el delito cometido sea contra un grupo de personas, pudiendo ser, un grupo de personas que no estén relacionadas entre sí, o que si estén relacionadas entre sí.

El sujeto pasivo dentro del delito informático es la persona o grupo de personas a las que se les ha realizado un perjuicio en su persona por medio de dispositivos electrónicos lo cuales pueden estar conectados por medio del internet, por lo cual es necesaria una profunda investigación para saber quién ha causado el delito.

Al ser el Estado el sujeto pasivo de un delito informático es muy prejudicial no solamente para el Estado como entidad gubernativa, sino también para los habitantes de dicho Estado, pues al haber transportado la documentación de las diferentes instituciones del Estado de libros y documentos para digitalizarlos y que puedan estar en la red electrónica,

[14] Balmaceda Hoyos. **Op. Cit.** Pág. 201.

por tal motivo, el que comete el delito, puede tener información clasificada, misma que se contienen en las bases de datos.

Al ser la persona jurídica el sujeto pasivo de un delito el sujeto activo puede tener toda la información de esta, ya sea confidencial o no, como lo pueden ser, puestos, nombres de empleados, salarios, proveedores, clientes, documentación intima del que hacer de la persona jurídica, perjudicando tanto a trabajadores, como a la persona jurídica directamente.

3.4 Sujeto pasivo del delito informático y su impacto en la sociedad

Al ser el sujeto pasivo la víctima en un delito informático requiere que el sujeto activo tenga conocimientos de informática, no obstante, para que una persona ser convierta en sujeto pasivo de un delito informático, no se requiera o necesita que la persona tenga conocimiento alguno sobre informática, pues puede ser perjudicado aun cuando él no haga uso de medios electrónicos o informáticos.

3.4.1 Formas que hacen que una persona pueda ser susceptible de convertirse en sujeto pasivo de un delito informático

La mayoría de las personas al crear un usuario electrónico para registrarse en las diferentes plataformas electrónicas, hacen caso omiso a las condiciones de uso, política de datos, política de cookies y política de privacidad que en ellas se encuentran, por tal motivo no están informadas.

Suele suceder que solo presionan el botón de aceptar, por motivo de que lo único que les interesa es poder utilizar determinada página web, en consecuencia de esto, no saben cuáles son los términos y condiciones que están aceptando y como va a ser manejada la información que están proporcionando al registrarse y al utilizar la plataforma, cabe destacar que si las personas no aceptan las condiciones de uso, así como las políticas de las plataformas que se quieran utilizar, la plataforma no aceptará tampoco su acceso a la misma, ni la utilización del servicio que ofrece.

Es importante que al momento de que una persona quiera registrarse en una plataforma electrónica se tome el tiempo para leer que es lo que se está estableciendo para poder utilizar el servicio prestado en las plataformas, pues todas estas condiciones de uso, políticas de datos, políticas de cookies, y políticas de privacidad, hacen las veces de un contrato, y al presionar el botón de aceptar, se está aceptando este contrato, teniendo como resultado consecuencias que pueden ser positivas o negativas.

Para el correcto conocimiento de a que se refiere las condiciones de uso, políticas de datos, políticas de cookies, y políticas de privacidad, se desarrollaran a continuación.

3.4.2 Condiciones uso dentro de una plataforma virtual

En todas las plataformas electrónicas existen las condiciones para poder registrarse en ellas, así como para poder acceder a la misma y utilizarla correctamente.

Se establece como se va a utilizar la información que proporciona el usuario que se pretende registrar, se da a conocer al usuario electrónica con los servicios que cuenta desde el momento en el que se registra como usuario del mismo, al mismo tiempo se hace saber cuáles funciones de la plataforma son pagadas o cuales son gratuitas, aquí también se establece lo que puede o no puede realizarse dentro de la plataforma y hace de conocimiento para las persona de qué tipo de información puede aparecer en la plataforma.

3.4.3 Política de datos

La política de datos es la que describe la información que se trata para respaldar productos y funciones que ofrece determinada plataforma electrónica, por lo que, si no se lee esta sección, no se sabe que es lo que sucede con la información que se está otorgando y que al ir utilizándola se seguirá proporcionando.

Por medio de esta sección se establece de qué forma se pueden utilizar los datos e información que se agregue en la plataforma, así como los que suba en ella y la información ya brindada.

Cabe destacar que en esta sección también se hace del conocimiento del usuario si al momento de utilizar el servicio, la plataforma recopila información proporcionada, pues en la mayoría de las plataformas que ofrecen un servicio lo realizan, pues es para ellos una forma de seguridad de que la pagina se está utilizando correctamente.

La información que suelen recopilar las distintas plataformas electrónicas son los nombres y apellidos del usuario, su edad, estado civil, nacionalidad, domicilio, número telefónico, imágenes, mensajes, archivos, las personas y grupos con los que se relaciona, esto el fin que busca es proporcionar un mejor servicio al usuario con relación a las cosas que tienen que ver con su estilo de vida, no obstante las personas se deben percatar que están brindando su información personal sin saber quién es el que la está recibiendo y manejando.

En esta sección también se establece que, si la aplicación o plataforma se utiliza en cualquier dispositivo electrónico, también va a recopilar los datos que en ellos se encuentran, por lo tanto pueden acceder a toda la información que se encuentra en el dispositivo, es decir, si se utiliza en una computadora, se recopilará datos de la computadora, si se utiliza en un teléfono inteligente, se recopilará datos del teléfono inteligente, así con todos los dispositivos con los que se utilice.

3.4.4 Política de cookies

Las cookies son conocidas como los pequeños fragmentos que existen en un texto los cuales se utilizan para almacenar información en los navegadores de la web, esto es como una memoria de las búsquedas realizadas en el pasado en los mismos dispositivos electrónicos.

La razón por la cual se utilizan las cookies es para ayudar a las personas a proporcionar, proteger y mejorar los servicios que ofrece la plataforma, para que conforme a las cosas que busquen las personas en la web, se guarde la clase de información que tiende a utilizar, eso es variado, puesto que como cada persona busca diferentes servicios e

informaciones en la web, esta se adapta a lo que el usuario como tal busca, sin importar que lo haga en diferentes dispositivos.

El fin de autenticación en las cookies, sirve para verificar la cuenta de los usuarios, y así poder determinar el momento en el que el usuario inicia sesión en la plataforma, por lo tanto, la persona puede utilizar los diferentes servicios que se ofrecen sin tener que iniciar sesión para cada servicio que quiera utilizar dentro de la misma plataforma o aplicación.

El uso de cookies se puede controlar de alguna manera, ya que el navegador o los dispositivos electrónicos pueden ofrecer dentro de las opciones de configuración, si se desea el uso de cookies en el navegador y la forma de eliminarlas, tendiendo en cuenta que algunas funciones de las plataformas se pueden ver desactivadas si sen limita el uso de las cookies.

3.4.5 Política de privacidad

Las políticas de privacidad en una plataforma electrónica, es la que le brinda protección al usuario, pues por medio de esta, el usuario puede limitar que aparezca en su usuario información propia que no quiere que vean los otros usuarios que utilicen también la plataforma.

Cabe destacar que este tipo de política está totalmente dirigida para el usuario, pues este no es un requisito que el usuario deba aceptar o aprobar para poder registrase y poder utilizar correctamente la plataforma, para poder proteger su información, la persona ya debe de haberse registrado dentro de la plataforma como un usuario de esta, por lo cual ya la puede utilizar.

En este apartado el usuario puede manejar que información es la que se puede mostrar y la que no se puede mostrar, así como, que usuarios pueden ver determinada información y cuales usuarios no pueden ver ese tipo de información, quienes se pueden comunicar con el usuario y quienes no lo pueden hacer, también se puede elegir qué información quiere el usuario guardar y cual quiere eliminar.

3.4.6 Casos que muestran el impacto social del sujeto pasivo

1. Es usual que lleguen personas a realizar trámites a los bancos del sistema guatemalteco, debiendo acreditar su personalidad a través de impresión dactilar, siendo a veces con tinta, frecuentemente los encargados de servicio al cliente brindan papel de reciclaje para que se limpien las manos, pero estos contienen información clasificada, como lo pueden ser, préstamos, pagos, depósitos, retiros, solicitudes de crédito, entre otras, en las cuales se leen información personal de los clientes.

   De caer en manos equivocadas, las personas de las que se da la información se pueden ver afectadas, hay que tomar en cuenta que los bancos no deben proporcionar información alguna sobre sus clientes, prestamos, créditos bajo ninguna circunstancia, por lo tanto, se ve irresponsabilidad por medio de los bancos.

2. Es frecuente que las personas que utilizan las redes sociales suban su información personal, como lo son sus nombres, fecha de nacimiento, domicilio, lugar de trabajo o estudios, número de teléfono, fotografías, gustos personales y más, algunos de estos no limitan sus usuarios por medio de las políticas de privacidad, pudiéndolo así ver y obtener su información cualquier persona que ingrese a su perfil.

   Al momento de realizar la creación de un usuario dentro de una plataforma electrónica, no es requerido que se haga de forma física, por tal motivo puede que una persona usurpe la información de otra persona, haciendo creer a los demás que es la persona a la que le usurpo su información, por lo tanto, esta forma de usurpación de identidad personal es muy común, pues se muestra toda la información a los demás usuarios.

3. Es común que las empresas hoteleras lancen propaganda del tipo de rifas y al momento en que las personas se acercan, les hacen de conocimiento que pueden entrar a una rifa para ganar estadías en hoteles lujosos o viajes, al momento que las personas aceptan les solicitan que lo único que tienen que hacer para poder entrar a la rifa es dar alguna información personal como lo es el nombre, edad y número

telefónico, a veces también solicitan esa misma información de conocidos, esto sin hacer del conocimiento de la persona que esa información otorgada es para su base de datos, por tal motivo luego la utilizan para ofrecer créditos, y servicios.

Eso afecta a las personas pues puede darse una fuga de la información, y esto puede caer en las manos incorrectas, estando así desprotegidas tanto las personas que brindaron su información personal, como también de las personas que se brindó su información.

4. En algunas ocasiones se pueden recibir en el correo electrónico un tipo de propaganda en la cual se anuncia que la persona que ha abierto el correo electrónico ha ganado gran cantidad de dinero, por lo cual se solicita que esta persona acceda a una página electrónica sugerida, al ingresar la persona a esta página, se le requiere que inserte sus datos personales.

   Se debe de tomar en cuenta que estos anuncios que llegan al correo electrónico son falsos, y al momento de que la persona abra el correo electrónico, ingrese a la página web sugerida o llene sus datos personales, brinda la posibilidad para que las personas puedan usurpar tanto su identidad, como también la información que poseen en su dispositivo electrónico.

3.5 La existencia de los delitos informáticos

La existencia de los delitos informáticos se ha debido al avance, así como al desarrollo que se llevado a cabo en el crecimiento de la tecnología, que si bien se ha convertido tanto en una forma de facilitar la vida de las personas y de ser un apoyo para ellos, en un perjuicio para todas las personas.

Al existir un vacío legal de la mayoría de los delitos informáticos dentro de la ley penal guatemalteca, se deja una brecha abierta para que personas malintencionadas puedan actuar mal sin tener una sanción por la acción cometida dentro del ordenamiento jurídico guatemalteco.

Dentro de los delitos informáticos existentes se puede mencionar:

3.5.1 La usurpación de identidad personal por medios informáticos

Este delito se comente cuando el sujeto activo utiliza la información personal del sujeto pasivo, para así engañar a los demás haciéndolos creer que el es la persona de quien se tiene la información.

3.5.2 Falsedad

Este delito se da cuando se crea algo dentro de la web que no es verdad o que no es el original.

3.5.3 Sabotaje

Es el delito que busca dañar la propiedad o generar perdidas a una persona mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.

3.5.4 Fraude

Es el delito que busca dañar mediante la manipulación de datos electrónicos para así poder obtener un lucro ilícito.

3.5.5 Amenazas

Este delito se da cuando por medio de la red electrónica y con el uso de dispositivos electrónicos se anuncia un mal futuro ilícito.

3.5.6 Calumnias

Este delito consiste en una acusación o imputación falsa que se hace contra otra persona, la cual se realiza en la red electrónica y con el uso de dispositivos electrónicos.

3.5.7 Pornografía infantil

Este delito busca utilizar a menores o incapaces con fines exhibicionistas o pornográficos, haciéndolo mediante las páginas web y propagándolo por medio de dispositivos electrónicos.

3.5.8 Secuestro de información

Es el delito por medio del cual se atrapa información y busca recibir el pago para que se rescate la información atrapada.

3.5.9 Alteración de documentos de clientes y fuga de información

Este delito se da cuando ejecutivos de ventas que ofrecen tarjetas de crédito y prestamos financieros, con el fin de recibir comisión ingresan documentación falsa.

CAPÍTULO IV

4. Derecho bancario

Es la rama del derecho que se ocupa de legislar y de estudiar el funcionamiento de los bancos.

4.1 Antecedentes

Asiria y Babilonia destacan por la creación de actividades y documentos que utilizaron para abordar a las actividades bancarias, principalmente se dio que en Babilonia en el Siglo VII a. C., crean el certificado de banco, letras de cambio, órdenes de pago y realizan la administración de bienes.

En el momento en que la moneda tomo un valor se convirtió en funcional, surgiendo así las necesidades de depositarlo, transportarlo y prestarlo, fue entonces cuando los comerciantes se dieron cuenta que estas eran formas de actividades lucrativas dándose así un precio para el depósito y el transporte y un interés por el préstamo.

En sus inicios, así como por largo tiempo, los primeros banqueros fueron exclusivamente judíos, que no eran alcanzados por las leyes de la iglesia y cuya principal función fue la de prestamistas, llegaron a establecerse en Lombardía para dedicarse a la banca, logrando operar en una gran extensión de territorio e incluso con algunos monarcas como Luis IX.

En el año 1400, en Génova, se empieza a utilizar la palabra banco misma que es para diferenciarse las actividades que realizaban, dando inicio a partir del Banco de San Jorge de Génova el que fue creado con sentido moderno en el año 1407 ya que anteriormente era conocido como Casa de San Jorge. Dicho banco se dividía en dos secciones: la primera, recibía depósitos; la segunda, surgió como una administración autónoma de la deuda pública de Génova, acordaba préstamos a los encargados de los impuestos y de la República excepto a los particulares.

En la actualidad las características esenciales alcanzadas en los sistemas bancarios y el desarrollo económico son variadas, y se deben en gran medida a la gran expansión. Los bancos hasta el día de hoy pueden encontrarse hasta en los pueblos más lejanos e incluyen a todas las clases socioeconómicas. Se pueden hacer diversas operaciones (cobros, pagos de documentos, impuestos, convenios, etcétera), así como, diversas obligaciones y modalidades operativas en las cuales buscan que se desarrolle su beneficio y así mismo la seguridad tanto de ellos como de sus clientes.

4.2 Normativa bancaria

La normativa bancaria se conoce como los estándares mínimos que la legislación le impone a las entidades financieras.

4.2.1 Banco

Los bancos son "sociedades mercantiles, trátese de Sociedad Nacional de Crédito o de Sociedad Anónima bancarias; cualquiera que sea su régimen de fundación, seguimiento, liquidación y naturaleza de los dueños, los bancos no son otra cosa que sociedades mercantiles; a partir de agosto de 1990, las bancas múltiples son, específicamente, anónimas."[15]

La referencia anterior hace saber que un banco está dentro del derecho mercantil, pues para la creación del mismo es necesario que este se conforme como una sociedad mercantil, esto sin importar la forma en cómo se lleve a cabo la creación del mismo, cabe destacar que dentro de las sociedades mercantiles existentes la que con mayor frecuencia es utilizada a nivel mundial para la creación de un banco es la Sociedad Anónima.

Tomando en cuenta la legislación guatemalteca se puede definir que un banco es una sociedad anónima especial cuyo objeto es la intermediación financiera que busca la

[15] Davalos Mejía Carlos Felipe. **Derecho bancario y contratos de crédito.** Pág. 109.

captación del dinero del público para así otorgar créditos, préstamos y financiamientos con un fin lucrativo.

Dentro de la legislación guatemalteca se define al banco como una sociedad anónima especial por la razón de que cuentan con los siguientes requisitos:

1. Tener una propia ley, la cual es el decreto 19-2002 Ley de Bancos y Grupos Financieros;
2. El objeto, el que es la intermediación financiera;
3. Un capital mínimo, que es de 148 millones en la actualidad pero que puede variar según resoluciones;
4. Existen acciones, la cuales deben ser nominativas;
5. Hay un trámite a seguir para la creación de un banco;
6. Tiene diversas denominaciones, como los son banco, banca, operaciones bancarias, banquero.

4.2.2 Objetivo del banco

Un banco realiza operaciones la cuales pueden ser activas, pasivas y de servicios, por tal motivo son estas operaciones las que realizan la relación que se crea entre el banco y los usuarios de este, por tal motivo el objetivo del banco es la intermediación financiera con un fin lucrativo.

Dentro del decreto 19-2002, Ley de Bancos y grupos financieros, en el artículo 3, se define el objeto del banco en Guatemala, la cual establece, "Los bancos autorizados conforme a esta ley o leyes especifica podrán realizar intermediación financiera bancaria, consistente en la realización habitual, en forma pública o privada, de actividades que consistan en la captación de dinero, o cualquier instrumento representativo del mismo, del público, tales como la recepción de depósitos, colocación de bonos, títulos u otras obligaciones, destinándolo al financiamiento de cualquier naturaleza, sin importar la forma jurídica que adopten dichas captaciones y financiamientos."

Por lo tanto, se da a entender que el objetivo del banco en la intermediación financiera bancaria, la cual se puede hacer de manera pública o privada, al momento de realizarse transacciones con dinero o que representen una cantidad monetaria.

En Guatemala existe el decreto número 19-2002, Ley de Bancos y grupos financieros, el objetivo de esta es la regulación de la estructura, organización y funcionamiento para realizar la creación, organización, fusión, actividades, operaciones, funcionamiento, suspensión de operaciones y liquidación de bancos y grupos financieros, así como al establecimiento y clausura de sucursales y de oficina de representación de bancos extranjeros.

4.2.3 Derecho bancario

Es el conjunto de normas, jurisprudencia, principios y doctrinas que regulan la estructura y funcionamiento de las entidades de crédito bancarias o entidades de depósito, así como también regula las operaciones realizadas con el público en general, incluidos sus clientes, con otras entidades de crédito financieras. Además de la banca oficial y privada, el derecho bancario se aplica a las instituidas como cajas de ahorro y las cooperativas de crédito.

Se integra de manera fundamental, por normas de derecho administrativo, mercantil, civil, financiero y fiscal.

En este sentido, cabe distinguir que se encuentra tanto en el derecho público, como en el privado, en el derecho público bancario por lo relativo a las normas constitucionales, administrativas y fiscales, y en el derecho privado bancario por lo relativo a las normas civiles y mercantiles.

Es una parte del derecho de las entidades de crédito, que se dedica a regular no sólo las entidades de crédito bancarias, sino también las entidades de crédito no bancarias o entidades de crédito de ámbito operativo limitado (como las entidades de financiación, las sociedades de crédito hipotecario y otras).

4.3 Secreto bancario

La Ley de Bancos y Grupos Financieros, decreto número 19-2002, en el Artículo 63, se encuentra regulado el secreto bancario, por lo que establece "Confidencialidad de operaciones. Salvo las obligaciones y deberes establecidos por la normativa sobre lavado de dinero u otros activos, los directores, gerentes, representantes legales, funcionarios y empleados de bancos, no podrán proporcionar información, bajo cualquier modalidad, a ninguna persona, individual o jurídica, pública o privada, que tienda a revelar el carácter confidencial de la identidad de los depositantes de los bancos, instituciones financieras y empresas de un grupo financiero, así como las informaciones proporcionadas por los particulares a estas identidades."

Por tal motivo, se puede comprender que el secreto bancario es la confidencialidad que los bancos le brindan a sus clientes, de la misma manera es la protección que los bancos les deben a las personas por medio de los trabajadores que en el laboren o que del mismo saquen beneficios, para que estos bajo ninguna forma puedan proporcionar información de sus clientes, información que se les proporcione, ni información sobre los tramites que se realicen dentro del banco.

El secreto bancario es también conocido como sigilo bancario, debido a que los trabajadores de los bancos deben de buscar la protección de los datos que se brindan y de los datos que se tienen, pues consiste en la protección que los bancos e instituciones financieras deben otorgar a la información relativa a los depósitos y captaciones de cualquier naturaleza, que reciban de sus clientes. Se entiende que esta información es parte de la privacidad de los clientes del sistema financiero.

Cabe destacar que existen entidades a las cuales se exceptúa el secreto bancario, pues estas tienen permitido solicitar información de los bancos e información que se intercambie entre los bancos y las instituciones financieras, las entidades que tienen excepción sobre el secreto bancario son la Junta Monetaria, el Banco de Guatemala, la Superintendencia de Bancos y la Superintendencia de Administración Tributaria.

Las entidades mencionadas en el párrafo anterior si bien pueden recibir la información que soliciten de los bancos tienen la prohibición de revelar la información que reciban, salvo que medie una orden de juez competente.

Si los directores, gerentes, representantes legales, funcionarios o empleados del banco dan a conocer información alguna sobre las actuaciones que se realizan adentro del banco o de alguno de sus clientes, así como si los miembros de la Junta Monetaria, funcionarios y empleados del Banco de Guatemala, de la Superintendencia de Bancos y de la Superintendencia de Administración Tributaria revelan información que sea sobre los bancos, se consideraran como falta grave y esto será un motivo para que se realice la inmediata remoción, esto sin perjuicio de las responsabilidades tanto civiles como penales que del hecho cometido se deriven.

Los clientes tanto de los bancos como de los grupos financieros tienen el derecho de privacidad de sus datos personales, así como de la información que brindan, movimientos, prestamos, créditos.

4.4 Transferencia electrónica

Se lleva a cabo cuando se traslada una cantidad de dinero de una cuenta a otra de manera electrónica.

4.4.1 Antecedentes

Para poderse lograr que en la actualidad se pueda realizar un pago, mediante una transferencia electrónica se tuvo que pasar por cinco pasos, los cuales fueron un avance dentro del derecho bancario al darles a las personas y a los clientes la forma de realizar pagos, cada uno de estos pasos aportó un sistema novedoso al derecho bancario, siendo estos:

a. El pago con moneda metálica. Al poder llegar a lograrse el pago con moneda de metal, se tuvo la necesidad de que el metal tuviera un valor como tal, por tal motivo se da determinada medida del metal.

b. El pago con moneda bancaria. Al momento de llegar al pago con moneda bancaria fue necesario que un sistema bancario realizara monedas o billetes los cuales para tener un valor monetario debe ser avalados por bancos o bancas centrales.
c. El pago con moneda cartular. Mediante esta forma de pago, se realizó un documento contable que debe ser avalado por los bancos del sistema en el cual se puede escribir la cantidad de dinero que se va a movilizar, este documento contable es conocido como cheque.
d. El pago con moneda plástica. Por medio de esta forma de pago, se realizó un documento plástico el cual debe ser avalado por los bancos del sistema, por medio del cual los clientes de determinado banco pueden obtener crédito en el uso de este la cual es conocida como tarjeta de crédito, o con la cual se puede hacer uso del límite de dinero depositado en la cuenta bancaria del propietario la cual es conocida como tarjeta de débito.
e. El pago sin moneda. Mediante esta forma de pago se logró que los bancos del sistema aprovechando el avance tecnológico pudieran realizar su propia plataforma por medio de la cual se pudiera prestar un servicio a sus clientes en el cual puedan movilizar el dinero de su cuenta con tan solo tener servicio a internet, esta forma en conocida como transferencia electrónica.

4.4.2 Definición de transferencia electrónica

La comisión de las Naciones Unidas para el Derecho Mercantil Internacional, conocida también por su nombre en inglés *United Nations Comission on International Trade Law* (UNCITRAL), define a la transferencia electrónica como toda transferencia de fondos en la que una o más operaciones del proceso que antes se desarrollaba sobre la base de técnicas documentales, se efectúa ahora mediante técnicas electrónicas.

Por lo tanto, la transferencia electrónica de fondos, la forma por medio de la cual los bancos se han facilitado tanto para ellos como también para sus clientes las operaciones bancarias activas y pasivas.

La transferencia electrónica de fondos aportó a que más personas se vieran en la necesidad de crear cuentas bancarias, por tal motivo los bancos se vieron mayormente beneficiados, pues en la actualidad las empresas, comercios, sociedades y entidades solicitan que sus trabajadores tengan una cuenta bancaria, y si no poseen una les facilitan a sus trabajadores por medio de una carta dirigida a determinado banco que esa persona labora en ese lugar por lo que se solicita que se le apertura una cuenta, esto con motivo de que les pueden pagar por medio de transferencia electrónica.

También es un beneficio para los clientes de los bancos, pues anteriormente se veían en la necesidad de hacer extensas colas para poder hacer depósitos, pagos, transferencias, sacar dinero, etcétera; pues ahora solo es necesario que tengas una cuenta dentro de un banco, solicitar un usuario electrónico, ingresar por medio del internet y un dispositivo electrónico a la página o aplicación del banco y realizar la operación bancaria necesaria.

4.4.3 La problemática de la transferencia electrónica

Con la transferencia electrónica surge una problemática que los clientes de los bancos deben de tomar en cuenta, pues al ser por medio de un dispositivo electrónico que se pueden efectuar las transferencias electrónicas, el cliente al momento de acceder a la plataforma del banco se convierte en un usuario, por lo tanto, se debe de comprender que al usuario no se le solicita su identificación para asegurarse que él es el propietario de la cuenta.

Por tal motivo se desarrolló junto con la utilización de la transferencia electrónica una serie de problemas que el banco y el usuario deben tener en cuenta, los cuales son conocidos como phishing, algunos de estos son:

a. La clonación de plataformas electrónicas. En algunas ocasiones los hackers incitan a la confusión de los usuarios, pues utilizan el nombre de la página web de determinado banco y le agregan alguna letra o símbolo que no se vea notorio, luego pagan anuncios en Google, así cuando las personas ingresan en Google el nombre de algún banco aparezca primero la página que ellos clonaron, con esto logran que al momento

de los usuarios ingresar su usuario y contraseña en la página clonada les quede a ellos cuales son y así pueden acceder a la cuenta de estos usuarios y realizar transacciones.

b. La usurpación de usuario y contraseña. En algunas ocasiones pueden llegar correos electrónicos que intentan hacer creer a las personas que es un correo enviado por algún banco, en ellos hace ver que es necesario que la persona introduzca su usuario y contraseña para validar alguna información, y al momento que la persona introduce sus datos ellos pueden saber cuáles son, y así poder realizar transferencias.

4.5 Formas de realizar fraude bancario

Con el uso de la transferencia electrónica de fondos se fue desarrollando el fraude con mayor frecuencia por motivo de que existe una vulnerabilidad al no ser de forma personal, logrando así múltiples formas para realizar el fraude bancario.

4.5.1 Prácticas deshonestas de los empleados

Este tipo de fraude si bien no es causado por el sistema electrónico este lo facilita, pues surge cuando que es el encargado de preparar la nómina, que es el comprobante el cual ordena que se pague a un proveedor, esta puede ser falsificada por motivo que el pago puede salir que se haga a favor de quien designe el empleado.

Este fraude se realiza al momento de hacer un retiro, si bien es un fraude esta transferencia se presenta ante el banco como verdadera y autorizada, pues ellos al tener acceso a las computadoras del banco pueden aprender de que forma pueden realizar las transferencias y evitar las medidas de seguridad para poder ejecutar el fraude.

4.5.2 Fraudes cometidos en terminales operadas por el cliente

Este tipo de fraude suele ejecutarse en el establecimiento en donde se encuentra el cliente y la computadora en la que lo realiza la que es el terminal que utiliza para

efectuarlo, esto se debe a que dentro del sistema de transferencias electrónicas los clientes pueden acceder a su cuenta dentro de la plataforma del banco.

Por lo tanto, el que activa las transacciones que se realizan es el cliente, por lo que, se puede dar como resultado el error por parte del banco, pues ya no es necesario que un banquero sea el intermediario de la transacción.

Por tal motivo tiene la posibilidad de haber fraudes, pues existen los llamado hackers que su objetivo es el desciframiento de la codificación, lo cual lo ha llevado a encontrar diversas formas de lograr su objetivo.

4.5.3 Fraude cometido por empleados del banco

Cuando los bancos contratan a sus empleados deben ser muy cuidadosos, debido a que en ellos se confía el manejo de clientes, transacciones y dinero, a esto se debe a que en la actualidad los bancos para contratar a una persona le realizan una investigación amplia para saber si es una persona honesta.

A pesar de estas grandes investigaciones existe la posibilidad de que haya empleados deshonestos, estos empleados deshonestos puedan realizar programaciones en la computadora de trabajo que les asignen, con objeto de acreditar dinero a su cuenta bancaria y eliminar cualquier rastro que pueda dejar dicha transacción.

Por lo tanto, si los bancos desean evitar que se les realice este tipo de fraude deben auditar las computadoras con frecuencia para ver si en ellas se encuentra instalado cualquier tipo de programas que permitan realizar fraude.

4.5.4 Fraude por intervención en el sistema de telecomunicación

Se debe comprender que los sistemas de telecomunicación pueden ser los teléfonos, computadoras, fax, tabletas, entre otros. Este tipo de aparatos están creados pensando en que su sistema de seguridad sea optimo y el que los usuarios de ellos necesitan, sin

embargo, si no se protege con un sistema codificado existe la facilidad de que al existir una comunicación con otro se pueda intervenir esta comunicación.

Al tener los bancos diversas formas de atención mediante los sistemas de telecomunicación, los bancos deben de proteger las comunicaciones con codificaciones para evitar este tipo de fraude, pues si no está protegido de esta forma puede darse a la facilidad de que la comunicación que se tiene entre el cliente y el banco sea intervenida.

4.6 Relación de derecho bancario con la usurpación de identidad personal por medios informáticos

La relación que existe entre el derecho bancario y el delito de usurpación de identidad personal por medios informáticos surge desde el momento en que los bancos empezaron a utilizar los sistemas de cómputo y se dio la digitalización de todos los datos de los clientes como la movilización del dinero.

Junto con la innovación de la facilitación de trabajo para los empleados de los bancos por medio de la digitalización de datos y el uso de computadoras nacen algunas formas de realizar fraudes por parte de empleados deshonestos.

Estas formas se relacionan con la usurpación de identidad personal por medios informáticos debido a que los empleados deshonestos de los bancos se hacen pasar por otra persona el cual es un cliente del banco, apropiándose de sus características, realizando el ilícito a través de una computadora dando como resultado el poder causar un perjuicio.

El surgimiento del secreto bancario trata de frenar que se dé la usurpación de identidad personal por medios informáticos, pues para evitar que se exista el fraude por parte de los empleados del banco busca la confidencialidad de operaciones bancarias por lo tanto los directores, gerentes, representantes legales, funcionarios y empleados de bancos, no pueden proporcionar información, bajo cualquier modalidad, a ninguna persona, individual o jurídica, pública o privada, que tienda a revelar el carácter confidencial de la identidad de los depositantes de los bancos, instituciones financieras y empresas de un

grupo financiero, así como las informaciones proporcionadas por los particulares a estas identidades.

Mas adelante volvió más fuerte la relación del derecho bancario con la usurpación de identidad por medios informáticos debido a que se creó la forma por la cual se realizan movimientos de las cuentas por parte de los clientes del banco, llegándose a la innovación y facilidad, dando como resultado la aparición de la transferencia electrónica.

El motivo por el cual la aparición de la transferencia electrónica se relacionó aún con mayor fuerza con la usurpación de identidad personal por medios informáticos es porque los clientes no necesitan una identificación que avale que son ellos los propietarios de una cuenta, por tal motivo algunas personas se hacen pasar por un cliente del banco ayudándose de la utilización de los medios informáticos realizándolo de diversas formas, haciendo como propias sus características y causándole un perjuicio.

CAPÍTULO V

5. Estudio de derecho comparado de Guatemala

El estudio de derecho comparado de Guatemala es la forma en la cual se evidencia como otros países protegen a sus habitantes de los ilícitos penales informáticos.

5.1 Antecedentes

El origen del derecho comparado viene desde Platón, pues el realizo la obra El primer estudio comparativo a las leyes, en esta obra se compara el derecho de las ciudades Estados griegas. En la obra mencionada no solo se toman en cuenta los derechos, sino además comprueba su eficacia, hacia lo que sería la Constitución ideal. Así mismo, Aristóteles realizo la comparación de las Constituciones de 153 ciudades dando también origen al derecho comparado.

El derecho comparado empezó a tomar mayor importancia desde el año 1900, por razón de que en este año se celebró el primer congreso internacional de derecho comparado, el cual conto con la participación de importantes figuras dentro del derecho comparado, Raymond Saleilles y Édouard Lambert, pues Raymond Saleilles era un profesional del derecho civil y con un espíritu comparativo, por motivo de que realizaba comparaciones del derecho civil con otros países, y Édouard Lambert siendo uno de los primero comparatistas puros y también siendo pionero de dar al derecho comparado una teoría y una metodología propia que proporcionaba fuerza para poder localizarlo de forma jurídica.

Sin embargo, el uso de la expresión de derecho comparado fue utilizada por primera vez en el Siglo XIX, por lo tanto, es una expresión moderna, en este momento se dejó claro que la comparación de las instituciones jurídicas merecía un enfoque sistemático, a fin de aumentar la comprensión de las culturas extranjeras y así fomentar el progreso jurídico de cada país.

Por tanto, el derecho comparado es una técnica que se utiliza para el estudio del derecho, la cual tiene la característica de busca instituciones o figuras jurídicas en distintos ordenamientos jurídicos, con el fin de profundizar el conocimiento que se tiene del ordenamiento jurídico propio.

El derecho comparado consiste en el estudio de las diversas instituciones jurídicas a través de las legislaciones positivas y que están vigentes en distintos países.

Pasos para un estudio comparativo

1. Se debe hacer la selección de un sistema jurídico.
2. Cuál es el sujeto o materia que se requiere comparar.
3. Delimitar el nivel de comparación.
4. Identificar cuales con las similitudes y cuáles son las diferencias.
5. Probar el cómo añadir determinado contenido dentro de la propia legislación es algo positivo y funcional.

5.2 Argentina

En Argentina el año 2018, se realizó una propuesta de proyecto de ley llamada, Ley de Suplantación de la identidad digital, bajo el registro S-2722/18.

El proyecto de ley fue realizado para que dentro del Código Penal argentino se añada un nuevo artículo, el cual se trata del delito de suplantar o apoderarse de la identidad digital, dicho artículo pasaría a ser el Artículo 139 ter, y según el proyecto de ley quedaría de la siguiente forma:

"Artículo 139 ter: Será reprimido con prisión de seis meses a dos años el que suplantare o se apoderare de la identidad digital de una persona humana sin su consentimiento, a través del uso de su nombre, apellido, foto o imagen, o cualquier otra característica que indefectiblemente la identifique como tal, utilizando para tal fin las Tecnologías de la Información y la Comunicación, con la intención de cometer un delito o causar un perjuicio a la persona cuya identidad se suplanta o a terceros.

La pena será de prisión de uno a cuatro años, siempre y cuando no configure un delito más severamente penado, en los siguientes casos:

a) Si se realizare de forma sostenida en el tiempo o de modo tal que obligare a la víctima a alterar su proyecto de vida;

b) Si la identidad creada, apropiada o utilizada fuere de una persona menor de 18 años.

c) Cuando el autor fuere un funcionario público.

El funcionario público, además de la pena de prisión, sufrirá inhabilitación especial por doble tiempo que el de la condena."

La razón por la cual se hizo la propuesta de ley es porque la identidad de una persona es lo que la va a acompañar para toda la vida convirtiendo a una persona en un ser único y distinto de los demás.

Tomando en cuenta de que en la legislación argentina en este momento posee un vacío legal en cuanto a la protección de la identidad virtual, la cual es tan importante como la real y, en la mayoría de los casos, mucho más sencilla de suplir de acuerdo con el avance tecnológico.

Haciendo notorio que en la actualidad las personas de todas las edades utilizan dispositivos electrónicos conectados al internet y tienen acceso a las redes sociales, es por lo tanto imperativa la creación de dicha norma para la protección de todos los argentinos.

Por lo tanto, al crear en el ordenamiento jurídico penal de Guatemala una norma que tipifique como una acción antijurídica, culpable y punible el suplantar, así como el apoderase de la identidad digital de una persona, sería un avance pues se estaría cumpliendo el principio constitucional de seguridad pues se estaría protegiendo a las personas y a su identidad personal.

5.3 Chile

En Chile el año 2015, se hizo una propuesta de proyecto de ley, llamada Ley de Suplantación de la Identidad en Redes Sociales, bajo el Boletín N°10411-07.

El motivo por el cual fue creado es que a nivel nacional el delito de usurpación de nombre a través de redes sociales ha aumentado en gran nivel, haciéndolo notorio en los datos policiales como en los datos del ministerio público que se han dado por medio de denuncias.

Dado que en Chile existe dentro del Código Penal el delito de usurpación de nombre el cual establece:

"Art. 214. El que usurpare el nombre de otro será castigado con presidio menor en su grado mínimo, sin perjuicio de la pena que pudiere corresponderle a consecuencia del daño que en su fama o intereses ocasionare a la persona cuyo nombre ha usurpado."

El articulo mencionado hace evidente que lo regulado es a un caso concreto, por tanto, no aplica cuando se comete por medio del internet o las redes sociales, por motivo de ser una regulación antigua y debe ser actualizado de acuerdo con el avance tecnológico.

Por tales motivos se realizó la creación del proyecto de ley, el cual propone que se incorpore al Artículo 214 del Código Penal chileno un inciso 2°, el cual establezca:

"Con la misma pena establecida en el inciso anterior se sancionará a quien suplante la identidad de una persona a través de las redes sociales existentes en Internet".

Por lo tanto, en Guatemala existe la clara importancia de que se realice la creación de una figura jurídica penal que establezca como delito y que sancione a quienes tomen como propio tanto el nombre como las características que son propias de otra persona por medio de internet, debido a que la perjudican, daría a las personas protección y seguridad, pues en este momento existe una laguna legal a lo que respecta el uso del internet y de las redes sociales.

5.4 México

En México en julio del año 2010, se promulgó una nueva ley, llamada Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Esta ley busca que se protejan los datos de las personas los cuales por diferentes razones están en posesión de particulares, imponiendo sanciones pues se busca como fin garantizar tanto la privacidad, como lo es el derecho a la autodeterminación informativa de las personas.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece:

"Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.

La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.

En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.

Artículo 8.- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.

El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los Artículos 10 y 37 de la presente Ley.

El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

Artículo 9.- Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

Artículo 10.- No será necesario el consentimiento para el tratamiento de los datos personales cuando:

I. Esté previsto en una Ley;
II. Los datos figuren en fuentes de acceso público;
III. Los datos personales se sometan a un procedimiento previo de disociación;
IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones

jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o

VII. Se dicte resolución de autoridad competente.

Artículo 11.- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.

El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

Artículo 12.- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.

Artículo 13.- El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

Artículo 14.- El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular sea

respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.

Artículo 15.- El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.

Artículo 16.- El aviso de privacidad deberá contener, al menos, la siguiente información:

I. La identidad y domicilio del responsable que los recaba;
II. Las finalidades del tratamiento de datos;
III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
V. En su caso, las transferencias de datos que se efectúen, y
VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

Artículo 17.- El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y
II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como

proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Artículo 18.- Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad.

No resulta aplicable lo establecido en el párrafo anterior, cuando el tratamiento sea con fines históricos, estadísticos o científicos.

Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares, o a la antigüedad de los datos, previa autorización del Instituto, el responsable podrá instrumentar medidas compensatorias en términos del Reglamento de esta Ley.

Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Artículo 20.- Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

Artículo 21.- El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable."

"Artículo 36.- Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.

El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos.

De igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

Artículo 37.- Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:

I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular."

En Guatemala no existe una ley, ni artículo alguno que busque directamente la protección de los datos personales, sin embargo, se creó en el año 2009 la Iniciativa 4090-2009 Ley de Protección de Datos Personales, pero la misma quedó solo como una iniciativa de ley, pues no fue tomada en cuenta.

Añadir la ley de protección de datos es positivo porque se busca que no se dé el mal manejo de los datos que las personas proporcionan a los particulares, por tanto, se convierte en funcional al bajar el índice de mal manejo de los datos de las personas.

5.5 Uruguay

Proyecto de ley de robo o suplantación de identidad y de estafa informática.

En Uruguay en marzo del año 2015, se entregó el proyecto de ley llamado Ley de Robo o Suplantación de Identidad y de Estafa Informática.

El proyecto de ley de robo o suplantación de identidad y de estafa informática busca que en el Código Penal Uruguayo se incorporen dos artículos, siendo los artículos añadidos, el Artículo 302 bis el cual su nombre sería robo o suplantación de identidad y el Artículo 347 bis el cual es estafa informática.

Atendiendo a esto, se propone que ambos artículos queden de la siguiente forma:

"Artículo 302 bis (Robo o suplantación de identidad) Comete robo o suplantación de identidad el que adoptare, creare, apropiare o utilizare, mediante la utilización de tecnologías o a través de Internet, de cualquier sistema informático, o medio de comunicación, la identidad de una persona física (aún fallecida) o jurídica que no le pertenezca. Este delito será castigado con dieciocho meses de prisión a ocho años de penitenciaría y con una multa de 160 a 3.200 unidades reajustables.

Cuando el autor asumiera la identidad de un menor de edad o tuviese contacto con un menor de edad, aunque mediare su consentimiento o sea funcionario público en ejercicio

de sus funciones o la víctima sea una persona con discapacidad, la pena será de cuatro a doce años de penitenciaría y con una multa de 160 a 3.200 unidades reajustables."

"Artículo 347 bis (Estafa informática) Comete estafa informática el que, mediante el uso de tecnologías, se valiere de cualquier manipulación engañosa de sistemas informáticos o de información en ellos contenida, para procurarse a sí mismo o a un tercero un provecho injusto en daño de otro, y será castigado con una pena de seis meses de prisión a cuatro años de penitenciaría y multa de 160 a 3.200 Unidades Reajustables."

El motivo por el cual este proyecto de ley fue creado es por el avance que se ha dado por parte de la tecnología, siendo el internet un medio que ofrece innumerables maneras de violentar la privacidad del usuario, existiendo un vacío legal en la ley penal con lo relativo a el robo o suplantación de identidad, estafas informáticas y otras modalidades fraudulentas.

Dándose cuenta por medio de las denuncias a las jefaturas de policía sobre delitos informáticos, así como haciendo notar el crecimiento que ha tenido el delito de suplantación de identidad informático, por tal motivo para otorgar protección y seguridad a los habitantes de Uruguay se realizó el proyecto de ley mencionado.

Ley de Protección de Datos Personales y Acción de Habeas data.

En Uruguay el 18 de agosto de 2008, fue publicada la ley de protección de datos personales y acción de habeas data, Ley N°18.331.

Esta ley busca la protección de los datos personales los cuales se registren en cualquier soporte, y que por tal motivo los haga susceptibles de tratamiento, ya sea si estos fueren públicos o privados.

Esta ley establece los derechos que tienen las personas con relación a los datos personales, siendo estos:

"Artículo 13. Derecho de información frente a la recolección de datos. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca:

A) La finalidad para la que serán tratados y quienes pueden ser sus destinatarios o clase de destinatarios.
B) La existencia de la base de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.
C) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.
D) Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud.
E) La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

Artículo 14. Derecho de acceso. Todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso solo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiera suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico.

Cuando se trate de datos de personas fallecidas, el ejercicio del derecho al cual refiere este artículo corresponderá a cualquiera de sus sucesores universales, cuyo carácter se acreditará por la sentencia de declaratoria de herederos.

La información debe de ser proporcionada dentro de los cinco días hábiles de haber sido solicitada. Vencido en plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, quedara habilitada la acción de habeas data.

La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.

La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales.

En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Artículo 15. Derecho de rectificación, actualización, inclusión o supresión. Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular.

El responsable de la base de datos o del tratamiento deberá realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde.

El incumplimiento de esta obligación por parte del responsable de la base de datos o del tratamiento o el vencimiento del plazo, habilitará al titular del dato a promover la acción de habeas data prevista en esta ley.

No precede la eliminación o supresión de datos personales salvo en aquellos casos de:

A) Perjuicios a los derechos e intereses legítimos de terceros.
B) Notorio error o falsedad.
C) Contravención a lo establecido por una obligación legal.

Durante el proceso de verificación, rectificación o inclusión de datos personales, el responsable de la base de datos o tratamiento, ante el requerimiento de terceros por acceder a informes sobre los mismos, deberá dejar constancia que dicha información se encuentra sometida a revisión.

En el supuesto de comunicación o transferencia de datos, el responsable de la base de datos debe notificar la rectificación, inclusión o supresión al destinatario dentro del quinto día hábil de efectuado el tratamiento del dato.

La rectificación, actualización, inclusión, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguna para el particular.

Artículo 16. Derecho a la impugnación de valoraciones personales. Las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa, que se base en un tratamiento automatizado o no de datos determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros.

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto.

La valoración sobre el comportamiento de las personas, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 17. Derechos referentes a la comunicación de datos. Los datos personales objeto de tratamiento solo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el

previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

El previo consentimiento para la comunicación es revocable.

El previo consentimiento no será necesario cuando:

A) Así lo disponga una ley de interés general.

B) En los supuestos del Artículo 9° de la presente ley.

C) Se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.

D) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.
El destinatario quedara sujeto a las mismas obligaciones legales y reglamentarias del emisor y este responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate."

CAPÍTULO VI

6. Presentación de resultados

La creación de la figura jurídica de la usurpación de identidad personal por medios informáticos genera protección y certeza jurídica a los habitantes de la República de Guatemala.

6.1 La estrategia nacional de seguridad cibernética

El avance en la tecnología ha creado necesidad de que las instituciones públicas y privadas desarrollen la seguridad informática.

6.1.1 Antecedentes

A partir del año 2018 se fue evidenciando el crecimiento y el avance que la tecnología estaba tomando a nivel nacional, lo cual llevo a las instituciones públicas a tomar medidas para proveer a los guatemaltecos seguridad informática.

La Superintendencia de Telecomunicaciones informó que es extensa la cantidad de números móviles existentes en Guatemala, por lo que se supone que un gran porcentaje de guatemaltecos en la actualidad cuenta con al menos un dispositivo electrónico o medio informático para comunicarse, esto les permite poder relacionarse de manera fácil a través de la cibernética con la sociedad, este movimiento otorga apoyo a la creación de grandes bases de datos.

Por lo que surgió el compromiso por parte del gobierno de Guatemala de fomentar el desarrollo tecnológico y la seguridad en el espacio cibernético para velar por la sociedad guatemalteca.

Por tal motivo la finalidad de la Estrategia Nacional de Seguridad Cibernética es resguardar la vida de los niños, niñas y adolescentes de las amenazas cibernéticas, autoridades del cuarto vicedespacho del Ministerio de Gobernación, presentó la

Estrategia Nacional de Seguridad Cibernética, que busca fortalecer la integridad de los internautas, así como la integridad, confiabilidad y disponibilidad de datos en el país.

6.1.2 Diagnostico Nacional de la Seguridad Cibernética

Analizando el estado actual de la seguridad cibernética tiene diferentes ejes importantes, por medio del estudio de cada uno de ellos se puede saber en dónde se necesita mayor refuerzo de seguridad, y la forma en la que se debe dar este refuerzo, entre estos ejes se puede mencionar, la infraestructura crítica, las tecnologías de información y comunicación, la investigación y respuesta a incidentes cibernéticos, la administración pública, el sector privado y financiero, la sensibilización y educación.

Infraestructura crítica es un eje, pues los principales objetivos de los actos delincuenciales relacionados el cibercrimen se encuentran en los crecientes y complejos ataques a las infraestructuras críticas, entre las que resaltan:

- La red eléctrica,
- La red de telecomunicaciones,
- La red de transporte,
- La red de infraestructura.

Las tecnologías de información y comunicación es otro eje, debido a que el internet ha incrementado en los últimos años en todo el territorio guatemalteco, abarcando todos los sectores sociales, pero el índice de preparación tecnológica es muy bajo, posicionando a Guatemala como uno de los países con menor preparación tecnológica a nivel mundial.

La investigación y respuesta a incidentes cibernéticos es otro eje, porque los mecanismos que estaban coordinados para dar respuesta a los incidentes cibernéticos dejaron de funcionar por motivo de falta de regulación legal, por lo que en la actualidad no existe entidad alguna que se encargue de su regulación a nivel nacional.

La administración pública es otro eje, dado que se hizo notorio que no existe ninguna gestión centralizada en el gobierno para la compra de tecnologías de información y

cibernética, por lo tanto, cada institución debe encargarse individualmente de ello, haciendo necesaria que una institución las coordine a todas.

El sector privado y financiero es otro eje, pues no existe una norma o gestión nacional que haya sido desarrollada o implementada con respecto a la gestión de incidentes cibernéticos, por lo que se evidencia la necesidad de crear la cultura de seguridad informática.

La sensibilización y educación son otro eje, debido a que resalto la preocupación en relación con la necesidad de un entendimiento compartido y definiciones comunes en seguridad cibernética, con el fin de fomentar la cultura de seguridad cibernética en todos los sectores del país.

Tomando en cuenta los diferentes ejes se puede evidenciar que todos están actualmente relacionados con la tecnología, por lo que el Estado al establecer una estrategia de seguridad informática realizo una división de importancia para validar los sectores más vulnerables y mayormente afectados.

6.1.3 Construcción de la estrategia

La elaboración de la construcción de la estrategia se realizó sobre la base de una visión nacional para lograr que se cumplan los objetivos que realicen la contribución de la seguridad en el espacio cibernético.

El proceso para la construcción de la estrategia considera cuatro fases:

1. La conformación de un Comité Ejecutivo Interinstitucional.
2. La definición y consenso de ejes y objetivos a alcanzar.
3. La validación de diagnóstico nacional, ejes estratégicos, objetivos y acciones concretas.
4. La formulación del documento final.

Dentro de la primera fase se realizó la integración de un Comité Ejecutivo Interinstitucional el cual fue conformado por los representantes del Ministerio de Relaciones Exteriores, Ministerio de la Defensa, Ministerio de Gobernación, Ministerio de Comunicación Infraestructura y Vivienda a través de la Superintendencia de Telecomunicaciones, Secretaría Técnica del Consejo Nacional de Seguridad y la Secretaría Nacional de Ciencia y Tecnología, a los cuales se les asigno la temática y metodología del proceso.

Así mismo se integraron mesas de trabajo las cuales estuvieron integradas por representantes de los diferentes sectores del país, como lo son las instituciones gubernamentales, financieras, infraestructuras críticas, sociedad civil, universidades y centros de investigación, esto con el propósito de fortalecer y retroalimentar la estrategia.

Dentro de la segunda fase se trazaron las metas y el plazo en que se tenían que llevar a cabo, fijando un período de tiempo del año 2016 al 2020, para que se cuente con un estrategia real y visible.

Fase final, dentro de esta fase se implementa la consulta pública, en la cual se le da la participación a la población en general, con las bases y criterios reunidos en su totalidad se logró consolidar el documento final.

6.1.4 Visión y principios generales

La visión que busca la Estrategia Nacional de Seguridad Cibernética es que la población que habita Guatemala se pueda dar cuenta de lo importante que es la seguridad cibernética, y que de la misma forma pueda entender, valorar y aprovechar cada medio informático efectivamente.

Entre los principios que rigen la Estrategia Nacional de Seguridad Cibernética están:

- La responsabilidad compartida. A todos les corresponde el ejercicio de la seguridad cibernética.

- Eficacia y proporcionalidad. Medidas adecuadas para garantizar el espacio cibernético seguro.
- Cooperación Internacional. La existencia de cooperación entre Estados para la transferencia, recepción e intercambio de información.

6.1.5 Ejes que conforman los objetivos para tomar acciones

La Estrategia Nacional de Seguridad Cibernética está compuesta por cuatro ejes estratégicos, diez objetivos y treinta y siete acciones que deben ser asumidas e implementadas por todos los sectores.

Ejes que derivan los objetivos de la estrategia:

A) Marcos Legales.

a) Adecuar el marco legal guatemalteco con un enfoque de prevención y manejo de riesgos cibernéticos para fortalecer la seguridad cibernética.
b) Promover la investigación para mantener niveles aceptables de seguridad cibernética.
c) Determinar una estrategia de divulgación que promueva la transparencia de la información.

B) Educación.

a) Promover la oferta educativa y formativa en seguridad cibernética que permita cubrir la demanda técnica y profesional en el país.
b) Desarrollar e implementar programas de educación para la formación y la investigación/desarrollo de la seguridad cibernética.

C) Cultura y Sociedad.

a) Gestionar la seguridad cibernética para la prevención, detección y relación ante amenazas del ciberespacio.
b) Establecer programas de sensibilización para contribuir en la gestión efectiva de riesgos y amenazas cibernéticas.

D) Tecnologías de Información.

a) Regular la protección de los sistemas de información digital en los sectores público y privado, para garantizar la continuidad de sus servicios.
b) Establecer las organizaciones de coordinación para implementar la seguridad cibernética nacional.
c) Diseñar un plan de protección nacional de infraestructuras críticas para fortalecer los planes de contingencia y de recuperación.

6.1.6 Gobernanza de la seguridad cibernética

La estrategia que desarrolla la gobernanza de la seguridad cibernética propone comités losa cuales deben ser orientados a la seguridad en el ciberespacio tanto a nivel estratégico como técnico que permita el correcto desarrollo para generar canales y espacios de intercambio de información, los cuales son necesarios entre el sector público y privado para actuar bajo un marco común de normas y lineamientos.

Comité Nacional de Seguridad Cibernética

Es el ente asesor del Consejo Nacional de Seguridad.

El Comité Nacional de Seguridad Cibernética es el encargado de incentivar y favorecer los espacios de coordinación de las políticas interinstitucionales e intersectoriales, así como de canalizar los esfuerzos en la vinculación de los planes estratégicos para poder lograr los objetivos de la Estrategia Nacional de Seguridad Cibernética.

Comité Técnico de Seguridad Cibernética

Es el encargado de reforzar las relaciones de colaboración, cooperación y coordinación entre los distintos sectores y partes interesadas en la seguridad cibernética, el cual está presidido por un delegado del Comité Nacional de Seguridad Cibernética.

El delegado del comité debe informar a los demás miembros del Comité Nacional de Seguridad Cibernética a través de reportes periódicos y avances en la implementación

de los planes de acción a nivel nacional, de la misma forma promoverá el intercambio de información y el desarrollo e implementación de los procesos y sistemas inoperables entre los diferentes sectores.

6.2 Coordinación Institucional

Se debe llevar una coordinación institucional a tener en cuenta que en Guatemala la comisión de un delito puede ser de acción o de omisión a las leyes del país, la usurpación de identidad personal por medios informáticos sería un delito por acción, debido a que el sujeto activo busca hacerse pasar por el sujeto pasivo, convirtiendo como suyas las características que identifican e individualizan al sujeto pasivo como tal, teniendo como objetivo causarle un perjuicio.

La comisión de la acción debe de reunir las características de un delito las cuales se establece que tiene que estar tipificado en la ley como un delito, tiene que ser una acción antijuridica, el actor debe ser culpable y debe existir una pena para el que lo ejecute, actualmente la usurpación de identidad personal por medios informáticos no se considera un delito, por no estar tipificado en la ley penal como delito.

El sujeto pasivo de la usurpación de identidad personal por medios informáticos debe denunciar esta acción que lo perjudica, pues es deber del Estado brindarles seguridad a los guatemaltecos, esta denuncia la puede realizar en la Policía Nacional Civil y/o en el Ministerio Público.

6.2.1 La Policía Nacional Civil

Tomando en cuenta la Constitución Política de la República de Guatemala establece como deber del Estado brindar a las personas la seguridad, se creó el decreto 11-97, Ley de la Policía Nacional Civil, en la que se establece que la seguridad interna de los guatemaltecos está a cargo de la Policía Nacional Civil, otorgándole así una labor investigativa.

Por tener una labor investigativa se pueden hacer denuncias a la Policía Nacional Civil, para realizar estas denuncias existen tres formas, una de ellas es ir a la estación de la Policía Nacional Civil más cercana, otra es hacer una denuncia confidencial llamando al número 1518 y la otra es llenando el formulario de denuncias que se encuentra en la página oficial del Ministerio de Gobernación de Guatemala, dentro del apartado servicios, dentro del apartado denuncias confidenciales 1518.

Al momento de hacer la denuncia se deben llenar requisitos para que esta sea de manera correcta, si la denuncia es presencial es necesario presentar el Documento Personal de Identificación, si la denuncia es por medio del número telefónico o por el formulario en línea, al ser una denuncia confidencial no es necesario que se presente el Documento Personal de Identificación. Dentro de la página de Ministerio de Gobernación, dentro del apartado servicios, dentro del apartado denuncias confidenciales 1518, se enseña que para hacer una denuncia se requiere ser breve y puntual, poner datos específicos de la incidencia y agregar imágenes o videos que puedan ser tomados como evidencia.

Posteriormente la Policía Nacional Civil debe emitir una constancia de la denuncia que se tomó y llevar un seguimiento del caso, al documento que la Policía Nacional Civil entrega a la fiscalía con el fin de iniciar las indagaciones se le llama parte policial.

Los encargados de realizar la investigación por parte de la Policía Nacional Civil es la Dirección Especializada de Investigación. Anteriormente cuando se denunciaba la usurpación de identidad personal por medios informáticos y el daño hacia el sujeto pasivo era un perjuicio económico, la Dirección Especializada de Investigación lo enviaba a su Unidad de Delitos económicos para su investigación.

En la actualidad dentro de la Dirección Especializada de Investigación existe la Sección de investigación Contra Delitos Informáticos, la cual es la encargada de investigar los casos denunciados acerca de la usurpación de identidad personal por medios informáticos.

En la actualidad la laguna legal existente para la acción maliciosa de la usurpar la identidad de una persona utilizando como medio para lograr su objetivo la tecnología, la persecución penal es inexistente pues no existe una conducta ilícita que la legislación penal existente sancione y por tal motivo se perjudica la seguridad de los guatemaltecos.

6.2.2 Ministerio Público

El Ministerio Publico es una institución de carácter penal, la cual tiene funciones autónomas, promueve la persecución penal, así mismo dirige e investiga los delitos de acción pública.

Tomando en cuenta que al Ministerio Público se le otorgan las facultades de dirigir la investigación de los delitos de acción pública, promover la persecución penal y velar por el estricto cumplimiento de las leyes del país, las personas que se ven vulneradas de sus derechos pueden presentar denuncias a dicha institución.

El Ministerio Público se encuentra en la Constitución Política de la República de Guatemala, la cual establece en su Artículo 251 que "El Ministerio Público es una institución auxiliar de la administración pública y de los tribunales con funciones autónomas, cuyos fines principales son velar por el estricto cumplimiento de las leyes del país. Su organización y funcionamiento se regirá por su ley orgánica. El jefe del Ministerio Público será el Fiscal General de la República y le corresponde el ejercicio de la acción penal pública."

Para realizar denuncias los agraviados pueden hacerlo de manera presencial, dentro del área metropolitana se debe ir a la Oficina de Atención Permanente la cual se atiende a toda hora y todos le días, la persona que hace la denuncia debe presentar su Documento Personal de Identificación y dar informe del hecho sucedido, si tiene evidencia puede aportarla.

Con el avance tecnológico en Ministerio Público creó un sistema electrónico con el cual los ciudadanos pueden hacer denuncias individuales, institucionales y quejas por atención en el servicio a través de su teléfono celular o una computadora con acceso a

internet, para poner una denuncia electrónica por medio del teléfono celular o tableta se puede sea descargar la aplicación llamada reportes MP, pero también se pueden hacer denuncias a través de la página oficial del Ministerio Público.

Para hacer una denuncia a través del sistema electrónico del Ministerio Público se requiere seguir con cinco pasos, los cuales son:

- Si el agraviado es ciudadano guatemalteco debe registrar el Código Único de Identificación el que lo encuentra en su Documento Personal de Identificación y su fecha de nacimiento, en caso de ser extranjero deberá registrar su número de pasaporte y país de emisión, con esta información se validaran sus datos.
- El usuario deberá registrar la información relacionada al hecho sucedido.
- El ciudadano deberá registrar la información relacionada a la fecha, hora, lugar y una narración descriptiva del hecho denunciado.
- Se debe describir las características de los objetos y/o documentos robados o extraviados.
- Se debe leer si la información está correcta, y de ser así se debe confirmar la información y enviarla.

Posteriormente de realizarse la denuncia, esta se debe enviar a la fiscalía de delitos informáticos, la cual debe de realizar la investigación necesaria y el fiscal encargado evaluará la solicitud ante juez competente.

6.2.3 Instituto Nacional de Ciencias Forenses

El Instituto Nacional de Ciencias Forenses es una institución con autonomía funcional e independiente que surge como consecuencia de la necesidad de unificar y fortalecer los servicios periciales forenses en Guatemala, mediante el desarrollo científico del trabajo que realiza como institución autónoma, garantizando la imparcialidad y confiabilidad de la investigación técnica científica, contribuyendo así al sistema de justicia.

Por motivo de ser una institución que está dedicada a los servicios periciales dentro del país, es necesario que este a la vanguardia y que los trabajadores de esta institución

sean capacitados frecuentemente, así como es necesario que la tecnología con la que realizan los peritajes sea de excelente calidad y funcionamiento.

Al existir delitos informáticos fue necesaria la capacitación y la adquisición de aparatos para realizar peritajes informáticos, por lo tanto, el Instituto Nacional de Ciencias Forenses ya tiene creado su equipo y está dotado de equipos para comenzar a trabajar análisis científicos en cómputo forense.

Las instituciones nacionales del gobierno y el Instituto Nacional de Ciencias Forenses ya cuentan con convenios que permiten solicitar a las grandes empresas mundiales que controlan las grandes bases de datos, el solicitar por medio de un proceso entre ellos, la información concerniente a un perfil, cuenta, blog o correo electrónico de una persona que está cometiendo un delito informático.

6.3 Phishing

Tomando en cuenta que en la mayoría de las veces que se ejecuta el phishing es con el objetivo que causar un perjuicio económico a las personas, siendo esta una forma por la que se realiza la usurpación de identidad personal por medios informáticos, por tal motivo las entidades bancarias y financieras deben estar preparadas y tener un plan de acción para proteger a sus clientes.

6.3.1 La Superintendencia de Bancos

La Superintendencia de Bancos es la encargada de promover la estabilidad y la confianza en el sistema financiero supervisado, siendo de reconocida credibilidad y prestigio, que realiza su trabajo y supervisión efectiva en forma eficaz, medible y conforme a estándares internacionales, aprovechando las tecnologías de información y comunicaciones, haciendo uso eficiente de los recursos disponibles, con personal calificado y comprometido con la institución y sus valores.

Por tal motivo, la Superintendencia de Bancos realiza una auditoria permanente en cada uno de los bancos, con esta auditoría vela por la estabilidad de cada banco del sistema,

dentro de la auditoria que realiza se encuentra como un punto la evaluación de riesgos informáticos, a través de esta evaluación ellos emiten observaciones y si se encuentra alguna alerta de phishing en contra de alguno de los bancos les anuncian y les fijan plazos para que estas sean atendidas.

6.3.2 El Banco de Guatemala

El Banco de Guatemala es el encargado de contribuir a la creación y mantenimiento de las condiciones más favorables al desarrollo ordenado de la economía nacional, para lo cual propiciará las condiciones monetarias, cambiarias y crediticias que promuevan la estabilidad en el nivel general de precios.

Por lo tanto, el Banco de Guatemala no puede tomar acción si se da phishing en algún banco privado, pues no está dentro de sus funciones, sin embargo, el Banco de Guatemala tiene un sistema de prevención en contra del phishing de manera interna.

Pasos que utiliza el Banco de Guatemala para prevenir el Phishing de forma institucional y de forma personal para sus trabajadores:

1. Se envían de manera periódica mensajes a los usuarios trabajadores informándoles sobre la seguridad informática.
2. Al momento que una persona ingresa a laborar dentro del banco por parte de una inducción que se les debe dar, incluye charlas sobre la seguridad informática.
3. De forma periódica se realizan unos laboratorios, en los cuales el departamento envía correos a los trabajadores que contienen una simulación de phishing, para ver que trabajadores caen, lo cual enseña a los trabajadores a sobre su seguridad informática.
4. En caso de verse afectada la seguridad del Banco de Guatemala los encargados de seguridad informática dentro del banco deben bloquear manualmente las direcciones atacantes.
5. Dentro del correo del Banco de Guatemala está instalado un botón para reportar al administrador, cual consiste en borrar el mensaje de la bandeja de entrada y enviar una copia al encargado de seguridad Informática para que este lo analice.

Forma de evitar que los trabajadores caigan en phishing:

1. Dentro del Banco de Guatemala se cuenta con mecanismos de bloqueo, llamado proxy, el cual filtra el contenido de internet y analiza todo el contenido navegado, bloqueando desde este sistema cualquier filtración de información.
2. Todos los equipos dentro del Banco de Guatemala cuentan con un antivirus instalado el cual evita que se descarguen virus o amenazas que existan.

6.3.3 Bancos del sistema nacional

El banco es una es una sociedad anónima especial cuyo objeto es la intermediación financiera que busca la captación del dinero del público para así otorgar créditos, préstamos y financiamientos con un fin lucrativo, por tal motivo tiene que otorgar a sus clientes seguridad y protección al momento de existir la relación entre cliente y banco.

Por tal motivo, todos los bancos del sistema deben contar con departamentos específicos de seguridad en contra de delitos informáticos, para de esta forma poder proteger a sus clientes.

CONCLUSIÓN DISCURSIVA

El problema detectado es la falta de regulación en la ley penal guatemalteca del delito de usurpación de identidad personal por medios informáticos, pues el Código Penal de Guatemala vigente en su Artículo 1, contiene el principio de legalidad, el cual establece que ninguna persona puede recibir una pena por hechos que no están calificados como delitos, también el Artículo 7, prohíbe la analogía lo que significa que no se puede crear figuras delictivas o aplicar sanciones utilizando la analogía, el Código Penal contiene un apartado de delitos informáticos, pero en este no se incluye a la usurpación de identidad personal por medios informáticos como un delito.

Por tal motivo es necesario que el Estado tome en cuenta que los guatemaltecos carecen de protección y seguridad informática en la utilización y manejo del ciberespacio al no estar regulada la usurpación de identidad personal por medios informáticos como un delito en la actual ley penal guatemalteca, para así poder cumplir el fin constitucional de proteger a la persona y con el deber constitucional de otorgar seguridad a la persona.

BIBLIOGRAFÍA

AMUCHATEGUI REQUENA, Griselda. **Derecho penal.** Estados Unidos. 2006. Oxford.

BALMACEDA HOYOS, Gustavo. **Estudios de derecho penal general.** Colombia. 2015. Ediciones nueva jurídica.

Banco de Guatemala. **Manual de procedimientos.** Guatemala.

BARRIOS OSORIO, Omar Ricardo. **Derecho e informática.** Guatemala. 2007. Ed. Mayté.

CABANELLAS DE TORRES, Guillermo. **Diccionario jurídico elemental.** Argentina. 2005. Ed. Heliasta.

DAVALOS MEJÍA, Carlos Felipe. **Derecho bancario y contratos de crédito.** México. 1984. Ed. Harla.

GARCÍA MAYNEZ, Eduardo. **Introducción al estudio del derecho.** México. 1984. Ed. Porrúa.

HERNÁNDEZ FUENTES, Jonathan Efraín. **Informática y derecho.** Guatemala, 2010.

https://www.20minutos.es/noticia/3247826/0/**delitos-usurpacion-identidad-internet-redes-sociales**-se-duplican-region-solo-5-anos/

https://www.adalidmedrano.com/**convenio-ciberdelincuencia-budapest/2017/**

https://www.debate.com.mx/prevenir/Cuidado-**El-robo-de-identidad-digital**-sigue-creciendo-20170606-0351.html

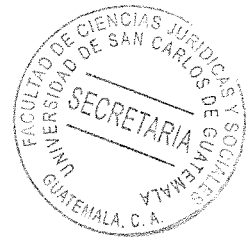
https://www.delitosinformaticos.com/09/2016/noticias/**delito-usurpacion-identidad-internet**

https://www.eleconomista.com.mx/politica/**14-tecnicas-para-robar-tu-identidad**-20170531-0038.html)

https://www.enciclopedia-juridica.com/**inicio-enciclopedia-diccionario-juridico**.html

https://www.es.sos-internet.com/**usurpacion-de-identidad-en-internet/**

https://www.legalitas.com/pymes-autonomos/actualidad/articulos-juridicos/contenidos/**La-usurpacion-de-identidad**



https://www.mingob.gob.gt/**estrategia-nacional-de-seguridad-cibernetica/**

https://www.muycomputer.com/2017/01/25/**robo-de-un-dispositivo/**)

https://www.oas.org/es/sla/ddi/docs/U4%20Ley%2018.331%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20y%20Acci%C3%B3n%20de%**20Habeas%20Data**.pdf

https://www.observatoriolegislativocele.com/**chile-proyecto-de-ley-suplantacion-de-la-identidad-en-redes-sociales-2015/**

https://www.observatoriolegislativocele.com/wp-content/uploads/Argentina-Proyecto-de-Ley-Suplantaci%C3%B3n-de-la-Identidad-Digital-2722-2018.pdf

https://www.repositorio.uchile.cl/handle/2250/135613

https://www.tecnologia.elderecho.com/tecnologia/privacidad/**usurpacion-identidad-redes-sociales**_11_585805001.html

https://www.vamosuruguay.com.uy/**robo-o-suplantacion-de-identidad-y-de-estafa-informatica/**

LÓPEZ GUARDIOLA, Samantha Gabriela. **Derecho penal I.** México. 2012. Ed. Red tercer milenio.

MARTÍNEZ CHACÓN, Karla Cristina. **Necesidad de regular jurídicamente el bien informacional.** Guatemala. 2006. Ed. USAC.

MARTÍNEZ PAZ, Fernando. **La construcción del mundo jurídico multidimensional.** Argentina. 2004. Ed. Advocatus.

Ministerio Público. **Manual de procedimientos.** Guatemala.

PALACIOS MOTTA, Jorge Alfonso. **Apuntes de derecho penal.** Guatemala. 1980. Ed. Gardisa.

PÉREZ LUÑO, Antonio Enrique. **Informática jurídica y derecho de la informática en España.** España.

Policía Nacional Civil. **Manual de procedimientos.** Guatemala.

Prensa Libre, el 2 de septiembre de 2018, página 17.

RAMÍREZ GAITÁN, Daniel Ubaldo. **Derecho bancario y bursátil.** Guatemala.

Real Academia Española. https://www.dej.rae.es/

ROMERO FLORES, Rodolfo. **Las conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa.** México. 2016. Ed. Universidad Autónoma de México.

Superintendencia de Bancos. **Manual de procedimientos.** Guatemala.

TÉLLEZ VALDÉS, Julio. **Derecho Informático.** México. 2008. ed. Mc Graw Hill.

VILLAZÁN OLIVAREZ, Francisco José. **Manual de informática I.** México, 2010.

ZAMORA ALVIZURES, José Carlos. **Implementación de la informática forense en la obtención de evidencia digital para combatir los delitos informáticos en Guatemala.** Guatemala. 2012. Ed. USAC.

Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, Guatemala, 1986.

Código Penal. Decreto 17-73, Congreso de la República de Guatemala, 1973.

Ley de Bancos y Grupos Financieros. Decreto 19-2002, Congreso de la República, 2002.