Universidad Estatal de Bolívar

Facultad de Jurisprudencia, Ciencias Sociales y Políticas.

Carrera de Derecho

Proyecto de trabajo de integración ccurricular previo a la obtención del título de abogada.

Título

Análisis del derecho a la privacidad, en base a los datos personales, en delitos cibernéticos, banco pichincha, año 2019.

Autora

Jennifer Stefania Montalvo Tualombo

Tutor.

Dr. Washington Javier Bazantes Escobar

Guaranda-Ecuador

2024

DECLARACIÓN DE AUTORÍA.

Yo, Dr. Washington Bazantes Escobar., en mi calidad de Tutor del Proyecto de Investigación, designado por disposición de Consejo Directivo, bajo juramento CERTIFICO: que la Sra. **JENNIFER STEFANIA MONTALVO TUALOMBO**, egresado de la Universidad Estatal de Bolívar, Facultad de Jurisprudencia, Ciencias Sociales y Políticas, Carrera de Derecho, ha cumplido con su trabajo de grado previo a la obtención del título de Abogada; con el tema: **"ANÁLISIS DEL DERECHO A LA PRIVACIDAD, EN BASE A LOS DATOS PERSONALES, EN DELITOS CIBERNÉTICOS, BANCO PICHINCHA, AÑO 2019"**, .mismo que ha cumplido con todos los requerimientos exigidos por la institución, siendo la misma de su propia autoría, por lo que se aprueba la misma.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado a hacer uso del presente, así como también se autoriza la presentación para la calificación por parte del jurado respectivo.

Atentamente,

DR. WASHINGTON BAZANTES ESCOBAR.

Tutora

DECLARACIÓN JURAMENTADA

NOTARÍA TERCERA
Msc. Ab. Henry Rojas Narváez
GUARANDA - ECUADOR

DECLARACIÓN JURAMENTADA

Yo; **JENNIFER STEFANIA MONTALVO TUALOMBO**, egresado de la Carrera de Derecho de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, bajo juramento declaro en forma libre y voluntaria que el presente Proyecto, con el tema: **"ANÁLISIS DEL DERECHO A LA PRIVACIDAD, EN BASE A LOS DATOS PERSONALES, EN DELITOS CIBERNÉTICOS, BANCO PICHINCHA, AÑO 2019"**, es de mí autoría, así como las expresiones vertidas en la misma, que se ha realizado bajo la recopilación bibliográfica tanto de libros, revistas, publicaciones, así como de artículos de la legislación ecuatoriana para el presente trabajo investigativo.

Atentamente.

JENNIFER STEFANIA MONTALVO TUALOMBO
Autor

NOTARÍA TERCERA
Msc. Ab. Henry Rojas Narváez
GUARANDA - ECUADOR

rio...

N° ESCRITURA 20250201003P01286

DECLARACION JURAMENTADA

OTORGADA POR: MONTALVO TUALOMBO JENNIFER STEFANIA

INDETERMINADA DI: 2 COPIAS

H.R.

Factura: 001-006- 000007860

En la ciudad de Guaranda, capital de la provincia Bolívar, República del Ecuador, hoy día dieciséis de Mayo del dos mil veinticinco, **ante mi Abogado HENRY ROJAS NARVAEZ, Notario Público Tercero del Cantón Guaranda,** comparece la señorita MONTALVO TUALOMBO JENNIFER STEFANIA, de estado civil soltera de ocupación estudiante, domiciliada en el cantón Caluma provincia Bolívar y de paso por este lugar, con celular número (0980894509), su correo electrónico es smontalvo.sofi@gmail.com , por sus propios y personales derechos, a quien de obligarse y de conocer doy fe en virtud de haberme exhibido sus documentos de identificación y con su autorización se ha procedido a verificar la información en el Sistema Nacional de Identificación Ciudadana; bien instruidas por mí el Notario con el objeto y resultado de esta escritura pública a la que procede libre y voluntariamente; advertido de la gravedad del juramento y las penas de perjurio, me presenta su declaración Bajo Juramento declara lo siguiente manifiesto que el criterio e ideas emitidas en el presente trabajo de investigación titulado **"ANÁLISIS DEL DERECHO A LA PRIVACIDAD, EN BASE A LOS DATOS PERSONALES, EN DELITOS CIBERNÉTICOS, BANCO PICHINCHA, AÑO 2019",** Es de mi exclusiva responsabilidad en calidad de autora, previo a la obtención del título de Abogada de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, Es todo cuanto puedo declarar en honor a la verdad, la misma que la hago para los fines legales pertinentes. HASTA AQUÍ LA DECLARACIÓN JURADA. La misma que elevada a escritura pública con todo su valor legal. Para el otorgamiento de la presente escritura pública se observaron todos los preceptos legales del caso, leída que le fue a la compareciente por mí el Notario en unidad de acto, aquella se ratifica y firma conmigo de todo lo cual doy Fe.

B.0884565

MONTALVO TUALOMBO JENNIFER STEFANIA

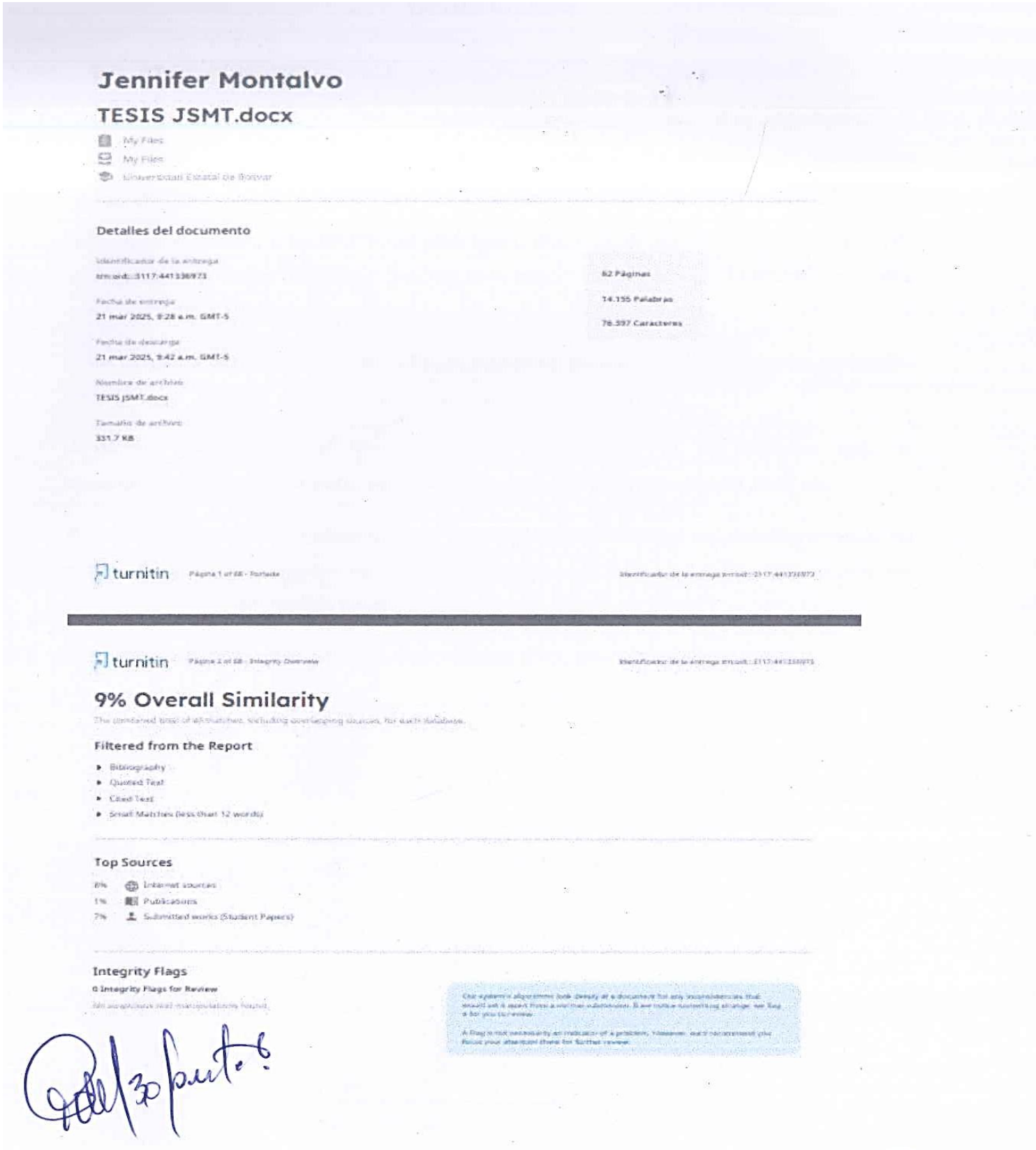
C.C. 0202121281

AB. HENRY ROJAS NARVAEZ

NOTARIO PUBLICO TERCERO DEL CANTON GUARANDA

EL NOTA....

REPORTE DE SIMILITUD DEL TURNITING.



Jennifer Montalvo

TESIS JSMT.docx

My Files

My Files

Universidad Estatal de Bolívar

Detalles del documento

Identificador de la entrega
trn:oid:::3117:441336973

Fecha de entrega
21 mar 2025, 9:28 a.m. GMT-5

Fecha de descarga
21 mar 2025, 9:42 a.m. GMT-5

Nombre de archivo
TESIS JSMT.docx

Tamaño de archivo
331.7 KB

82 Páginas

14.155 Palabras

76.597 Caracteres

turnitin Página 1 of 88 - Portada

turnitin Página 2 of 88 - Integrity Overview

9% Overall Similarity

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 12 words)

Top Sources

8% Internet sources
1% Publications
7% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

DERECHOS DE AUTOR

Yo; Jennifer Stefania Montalvo Tualombo, portador de la Cédula de Identidad No 0202121281, en calidad de autor titular de los derechos morales y patrimoniales del Trabajo de Titulación: **Análisis del derecho a la privacidad, en base a los datos personales, en delitos cibernéticos, banco pichincha, año 2019.,** Modalidad Proyecto de Investigación, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo/autorizamos a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El (los) autor (es) declara (n) que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Jennifer Stefania Montalvo Tualombo

Autora

DEDICATORIA

Dedico este trabajo a mis padres, Carmen Tualombo y Luis Montalvo, quienes me han acompañado, apoyado a lo largo de toda mi vida, y por supuesto de mi carrera universitaria, nunca se rindieron a pesa de las dificultades que el destino tenía para mí.

A mi hija Valentina, a mi sobrino Jeydan quien desde su llegada dio un giro inesperado mi vida, regalándome sonrisas y fuerzas para seguir con mi vida, mi carrera y con ella, cada logro en mi vida es para ellos.

A mi hermana Fernanda y hermano Lucio a quienes me han ayudado incondicionalmente en este largo viaje dándome fuerzas, valentía para no rendirme.

A mi apoyo incondicional Alexander quien estuvo para mí, sin importar nada, le agradezco mucho por ser parte de mi vida y ayudarme a ser mas fuerte cada día.

Por último, dedico a mis estrellas mas iluminadas en el cielo, a mi abuelita querida mi madrecita, a mi mejor amigo que desde su partida jamás me han dejado sola, siempre me estuvieron cuidando, en mis peores batallas.

Para cada una de ustedes, les agradezco mucho y los amo con toda mi vida.

AGRADECIMIENTO

Quiero agradecer a Stalin por estar para mi sin importar el tiempo o la distancia.

A mis hermanas Amalia y Alicia quienes me ayudaron cuidando y manteniendo a salvo mi vida y a mi hija.

A mis amigos incondicionales, porque a pesar de la distancia que nos separa siempre sentí su presencia junto a mí.

A todos los docentes con los cuales recibí clases, gracias por toda su paciencia, espero hacerlos sentir orgullosos de haber sido una de sus alumnas.

A la Universidad Estatal de Bolívar, por haberme abierto las puertas para ser estudiante y permitirme formarme como el profesional en el área de derecho.

A todos ustedes infinitas gracias.

INDICE.

CAPITULO I: PROBLEMA

1.1. Tema.

Análisis del derecho a la privacidad, en base a los datos personales, en delitos cibernéticos, banco pichincha, año 2019.

1.2. Resumen.

El internet se ha convertido en una red amplia de información, debido a su impresionante abastecimiento de datos que podemos obtener por este medio, es decir, llegar a formar una biblioteca virtual a nivel mundial, ha ido evolucionando en grandes formas, ya sean negativas o positivas, donde pueden romper cualquier tipo de limitaciones ya sean de tiempo o incluso de espacio. Los delitos cibernéticos son actividades delictivas donde estas son realizadas por medio de una computadora para poder manipular o acceder a datos de forma ilícita.

Debemos tomar en cuenta que los ataques cibernéticos no muchos son al azar, sin embargo, estos son más dirigidos a lo que son empresas, a las personas, a los diferentes sectores gubernamentales, entre otros. Estos delitos generan lo que es un impacto negativo ante la sociedad, existiendo la amenazas a empresas comerciales e individuales, las empresas que son encargadas de la seguridad cibernética introducen múltiples perímetros como la firewalls, detección y respuestas de amenazas. Es muy importante que el derecho proteja a los usuarios que son víctimas de estos delincuentes cibernéticos o ciberdelitos, sobre todo a la identidad que en muchos casos es vulnerado, ya que todos nos encontramos dentro de este fenómeno, donde la jurisdicción y la competencia tiene un papel muy importante dentro de esto que es el debido sancionatorio de cualquier tipo de actitud índole que se realice por estos medios informáticos.

Por otro punto la criminología y la victimología nos dan conocimientos e ideas aplicables en instancia de áreas de seguridad, política criminal y los derechos humanos, en caso de abordajes estratégicos tenemos a los casos penales, priorizando a juicio y teniendo responsabilidades penales.

Palabra clave.

Ataques cibernéticos, inteligencia artificial (IA), ciberdelincuentes, phishing, malware

1.3.Abstract.

The internet has become a wide network of information, due to its impressive supply of data that we can obtain by this means, that is, to form a virtual library worldwide, it has been evolving in great ways, whether negative or positive, where they can break any type of limitations, whether of time or even space. Cybercrimes are criminal activities where they are carried out by means of a computer to be able to manipulate or access data illicitly.

We must take into account that not many cyberattacks are random, however, these are more directed at companies, people, different government sectors, among others. These crimes generate what is a negative impact on society, there are threats to commercial and individual companies, companies that are in charge of cybersecurity introduce multiple perimeters such as firewalls, detection and threat responses. It is very important that the law protects users who are victims of these cybercriminals or cybercrimes, especially the identity that in many cases is violated, since we are all within this phenomenon, where jurisdiction and competence have

a very important role within this, which is the due sanctioning of any type of attitude that is carried out by these computer means.

On the other hand, criminology and victimology give us knowledge and ideas applicable in the areas of security, criminal policy and human rights, in case of strategic approaches we have criminal cases, prioritizing trial and having criminal responsibilities.

Key words

Cyberattacks, artificial intelligence (AI), cybercriminals, phishing, malware.

1.4.Introducción.

Los delitos cibernéticos o también conocidos como los ciberdelincuentes pueden llegar a ser personas común y corrientes se puede dar desde cualquier punto, desde cualquier lugar del mundo, a cualquier hora, minuto o segundo, desde cualquier dispositivo electrónico y con un poco de información informática, debemos tener en cuenta que la seguridad cibernética es muy importante en las empresas tanto públicas como privadas, en esta presente investigación se hizo énfasis al Banco Pichincha, en el año 2019 a partir de la pandemia del Covid-19 a raíz de esto se incrementaron sistemas informáticos para poder manejarse con total normalidad las cuentas de los usuarios, en el mismo año el ecuador quedo desprotegido de la seguridad cibernética, siendo un punto fijo para delincuentes cibernéticos, tratando de jaquear o ingresar al sistema bancario, por lo tanto la entidad financiera quedo sin sistema donde dieron a conocer que están en "mantenimiento".

Al momento de ser víctimas de estos delitos, debemos denunciar correctamente a las autoridades correspondientes, ya que estos delitos se encuentran tipificados en el Código Orgánico Integral Penal actualmente vigente, es importante también, implementar diferentes medidas de seguridad en los dispositivos electrónicos donde tengamos información delicada e importante como lo es nuestra banca móvil, Gmail, etc. En muchas ocasiones cuando somos víctimas es por error propio "error humano" y no es solo un error de las grandes empresas, recordemos que vivimos en la era de la tecnología, cada vez va

mejorando hasta el punto de que hoy en día la inteligencia artificial (IA) puede tener una conversación normalmente con una persona, teniendo ventajas y desventajas, como llegar al punto de vulnerar nuestros derechos, nuestra seguridad jurídica e informática.

En la actualidad o conocida como la era digital, los delincuentes se aprovechan de esta gran transformación en línea, para poder buscar puntos débiles y ataca como las redes infraestructurales y sistemas informáticos, a causado una enorme repercusión económica y social no solo en el Ecuador si no a nivel mundial, los ciberdelitos no conocen fronteras, los delincuentes, las víctimas, las infraestructuras técnicas, resulta ser muy problemático al momento de hacer una investigación o dar a conocer acciones jurisdiccionales.

Los delitos cibernéticos es un tema muy amplio esta se considera actividades ilegales, donde se tiene acceso al internet por medios de sus dispositivos electrónicos y redes informáticas, alterando contra la confidencialidad de los datos tanto personales como comerciales con finalidad de sustraer información con la que se pueda suplantar la identidad o llagar al punto de pedir rescates o recompensas, estos ciberdelitos pueden llegar a perpetuar por medio de individuos o grupos organizados para robar los activos de personas ya sea de forma individual, los bancos, las empresas, entre otros, utilizando técnicas avanzadas. Por otro lado, los delitos informáticos en el derecho son conocidos también como una conducta, típica, jurídica antijuridica y culpable, la tecnología es un medio para ocasionar lesiones o poner en peligro la libertad informática, llegando a afectar la confidencialidad, integridad y disponibilidad de redes y datos.

1.5. Planteamiento del problema.

El tema sobre los delitos cibernéticos se volvió controversial en el año 2019 pero en el 2020 cogió más fuerza, va de la mano junto con la tecnología que ha ido evolucionando a nivel mundial, donde facilita la convivencia y la transmisión de información, la

tecnología incluso ayudando a la ciencia, la medicina, el comercio, a las macro o microempresas, trayendo consigo sus beneficios y sus consecuencias.

¿Si habiendo normas, leyes y reglamentos vigentes en el ecuador, encargadas de regularizar la seguridad cibernética, por qué motivo existe una vulneración en grandes instituciones como en este caso el Banco Pichincha, perjudicando la identidad y la seguridad de los ciudadanos siendo así víctimas de aquellos delitos?

1.6. Formulación del problema.

¿Qué es el delito cibernético?

Entendemos por delito cibernético o ciberdelitos a las actividades ilegales o delictivas, estos se enfocan en dispositivos electrónicos y redes informáticas, llegando a actuar con mala fe con un fin económico.

¿Qué es el robo de identidad?

El robo de identidad es cuando una persona llega a suplantar a otra ya sea una persona natural o jurídica, este robo de identidad se da por medio de comunicaciones digitales

¿Cuál es el problema de esta investigación?

Tenemos en cuenta que los ataques cibernéticos son recurrentes en el país como, la estafa en línea a posibles víctimas y generar beneficios económicos con mala fe, el robo de datos personales e incluso datos de cuentas bancaria.

¿Cuáles son los principales tipos de delitos cibernéticos?

Dentro de los delitos cibernéticos podemos encontrar: Malware, Ransomware, Robo de identidad, Phishing, Pharming, Sniffing, Ciberacoso, Ciberterrorismo, Spyware.

1.7.**Hipótesis.**

¿Cómo los delitos cibernéticos afectan a Instituciones bancarias en este caso al Banco Pichincha, vulnerando así su sistema de seguridad cibernético?

1.8.Variables.

1.8.1. Variable independiente.

¿Delito Cibernético?

1.8.2. Variable dependiente.

Los delitos cibernéticos como el robo de datos personales y de cuentas bancarias, siguen aumentando en el país, causando daños a las posibles víctimas perjudicando su identidad y desconfiando de la seguridad cibernética.

1.9.Objetivos.

1.9.1. Objetivo general.

Analizar los métodos de recolección de evidencias y sus responsabilidades legales.

1.9.2. Objetivos específicos:

- Estudiar el marco jurídico ecuatoriano relacionadas con los delitos cibernéticos y sus aplicaciones.
- Conocer que derechos se vulneran cuando son víctimas de un delito cibernético.
- Aplicación de entrevistas sobre el delito cibernético en robo de datos personales.

1.10. Justificación.

En el estado ecuatoriano contamos con normas, leyes y reglamentos, donde se sanciona a las personas que lleguen a cometer cualquier tipo de delito cibernético, con una pena

privativa de libertad de uno a tres años, es decir, a medida que tecnología va avanzando, muchos de los sistemas de seguridad en diferentes instituciones se van vulnerando, sin embargo, nuestra legislación también va tomando diferentes medidas de seguridad como las sanciones con el único fin de prevenir estos delitos cibernéticos, estas actividades ilegales como el robo de datos personales o incluso el robo de identidad se encuentra regularizado en el Código Orgánico Integral Penal (COIP) y por supuesto en la Ley Orgánica de Protección de Datos Personales, junto de la mano con la Constitución de la República del Ecuador (CRE).

Es de gran ayuda tener una colaboración tanto en el sector público como en el sector privado para poder reforzar la seguridad cibernética, teniendo en cuenta que los delitos cibernéticos son acciones ilegales donde es utilizado la tecnología para ejecutar lo que es fraude, robo de datos, ataques informáticos y otras actividades delictivas, para que es importante esta investigación, pues bueno esta investigación tiene como finalidad ver la evolución de la tecnología, de los ciberdelitos, los tipos de delitos que podemos encontrar, no solo en el ecuador, tener más conocimientos en otros países, que medidas podemos tomar para no ser víctima de estos delitos, es decir, como podemos prevenir algún tipo de robo y estar actualizados en estos temas.

Este proyecto de investigación será de gran importancia dentro del debate académico y social poniendo como principal la protección de los derechos de los usuarios en las instituciones financieras como lo es el Banco ´Pichincha, esto se hace con el fin de garantizarnos seguridad cibernética a nuestros datos personales y no habiendo ninguna vulneración en el sistema.

CAPITULO II: MARCO TEORICO.

2.1. Marco histórico.

La tecnología se ha incrementado en todo el mundo teniendo sus beneficios como también sus contras

Los delitos cibernéticos en el ecuador empiezan a partir del siglo XXI, cuando el estado ecuatoriano empezó a involucrarse más con la tecnología de la información y sobre todo la comunicación, se podría decir que los delitos cibernéticos se mantenían al margen de los delitos más conocidos como el fraude en línea afectando a lo que es a las microempresas, como sabemos el incremento de la tecnología ha avanzado hasta el punto de llegar a tener una conversación normal con un ser humano, por medio de la tecnología e internet los ciberdelincuentes incrementaron medios de ataques como el phishing, malware, el robo de datos personales.

En respuesta a la creciente amenaza, Ecuador ha implementado diversas medidas para combatir los delitos cibernéticos. En 2012, el país promulgó la Ley Orgánica de Comunicación, que incluyó disposiciones para la protección de datos personales y la ciberseguridad. Posteriormente, se crearon unidades especializadas dentro de la Policía Nacional y la fiscalía general del Estado para investigar y perseguir estos delitos. A pesar de estos avances, los desafíos persisten debido a la rápida evolución de las técnicas criminales y la necesidad de una mayor cooperación internacional. Hoy en día, Ecuador continúa desarrollando su marco legal y fortaleciendo sus capacidades tecnológicas para proteger a sus ciudadanos en el entorno digital.

2.2. Marco teórico.

Este análisis se enfoca más en el marco teórico donde se darán a conocer los conceptos sobre el delito cibernético, responsabilidades legales, la inteligencia artificial (IA), las

vulneraciones que ha tenido el banco pichincha desde el año 2019, la superintendencia de bancos.

2.2.1. Responsabilidades legales sobre los delitos cibernético.

2.2.1.1.Sanciones penales sobre los delitos cibernéticos.

Como tenemos en consideración las actividades ilegales o delitos cibernéticos se pueden dar desde cualquier medio electrónico, como en muchos casos el robo de identidad e incluso el robo de datos personales causando daño a las posibles víctimas y así creando un beneficio económico para estos ciberdelincuentes, los delitos como la suplantación de identidad y en este caso el robo de datos personas, por medio de los dispositivos electrónicos y el avance de la tecnología estos delitos han ido aumentado cada día y se encuentra entre uno de los nuevos delitos.

Recordemos que en el año 2019 con lo que fue la pandemia del COVID 19 en estas fechas en el ecuador se dio a conocer varios delitos cibernéticos, el más comunes era la suplantación de identidad relacionado o en base al robo de datos personales, pero recordemos también que en el año 2020 el ecuador se quedó sin ningún respaldo del sistema de seguridad informática, causando así una gran inquietud e inseguridad por parte de la sociedad.

En el Código Orgánico Integral Penal (COIP), establece a estos delitos con su respectiva sanción.

En el artículo 190 nos establece sobre las apropiaciones fraudulentas por medios electrónicos, es decir, las personas que lleguen a cometer fraude utilizando, los diferentes tipos sistemas informáticos como las redes electrónicas o incluso los medios de comunicación, para poderse apropiar de un bien ajeno, ya sean valores o derechos, sobre sus datos personales, llegando así a perjudicar a una persona o incluso a terceros, en

beneficio económico ya sea así mismo, por medio de alteraciones, modificaciones, manipulaciones con el funcionamiento de la redes o equipos tele comunicativos, según lo establecido en la ley, será sancionado con un pena privativa de libertad de uno a tres años.

2.2.1.2.Protección de los derechos de la víctima sobre estos delitos.

La Constitución de la Republica del Ecuador (CRE), se encuentra vigente desde el 2008 donde nos establece como reparación a las víctimas de estos delitos cibernéticos, en el Artículo 77-78 del Código Orgánico Integral Penal (COIP).

Art. 77. Nos establece sobre la reparación integral, que nos quiere decir esto, que esta reparación consiste en la dar una solución ya sea de manera objetiva o incluso simbólica, donde se pueda restituir el daño de la manera más posible, sobre la situación de lis hechos fundados y llegue a satisfacer a la víctima, llegando a poner un fin a las infracciones que se han cometido, toda su naturaleza y su cuantía deberán depender del nivel de daño ocasionado al bien jurídico.

Art. 78. Dentro de los mecanismos de reparación no se pueden excluir formas de reparación de forma individual o incluso colectivas. Nos establece también sobre las indemnizaciones por daños inmateriales y daños materiales, refiriéndose así a la compensación por cualquier tipo de perjuicio que este derivado a una infracción penal, donde esta puede ser relevado de manera económica.

Por otra parte, encontramos al debido proceso en el Art 76 de la Constitución de la Republica del Ecuador, es decir, se utiliza en todos los procesos que tengan un derecho incluso obligaciones de cualquier orden, tendrán derecho un proceso digno y una defensa justa.

2.2.1.3. Derechos de los usuarios sobre sus datos personales.

Todas las empresas y los empresarios que están a cargo de los datos de cada usuario deben de respetar cada uno de los derechos de estas personas, y sobre todo facilitar sus servicios, también es importante que los usuarios tengan conocimientos sobres sus derechos.

Según la Ley Orgánica de protección de datos personales, nos establece en el capítulo I sobre los derechos, a quien va dirigido, que derechos se protegen y sobre todo bajo que autoridad quedan a cargo, desde el articulo 13 hasta el 20 y del artículo 22. La normativa especializada nos da a conocer que debe estar normado en ejercicio de la, libertad de expresión, gestión de riesgos, los desastres naturales y defensa de estado, estos datos deberán tener autoridades administrativas y judiciales.

2.2.1.3.1. Derecho a la información.

Este derecho sobre el acceso a la información es también conocido como un derecho fundamental dentro del sociedad, con el paso de la evolución, de su era digital. No establece que todos los ciudadanos sin importar su condición tienen derecho de solicitar y a recibir información por las instituciones incluso por las partes gubernamentales. El derecho a la información es considerado como parte del derecho a la libertad de expresión, es un derecho fundamental ya que es encargado de proteger la libre difusión y por supuesto el acceso a la información, pudiendo así entrar a documentos o incluso acceder a lo que son datos personales, ya sea por medio de entidades ya sea públicas o incluso privadas. La o el titular de los datos personales tiene derecho a ser informado basándonos en el principio de trasparencia y lealtad o cualquier otro medio como los fines del procedimiento, la base legal, el tipo de tratamiento, el tiempo que se puede obtener, la trasparencia, sus datos, su identidad, el titular de derechos, etc.

2.2.1.3.2. Derecho de acceso.

En este derecho sobre el acceso a la información es también conocido como el derecho de una persona para poder buscar y sobre todo adquirir información, es decir, puede

acceder, procesar, usar, analizar y por supuesto distribuir información pública, por medio de este derecho se puede acceder a lo que es el tratamiento de datos personales, este derecho nos garantiza, transparencia, lo que es rendición de cuentas y sobre todo la participación.

El o la titular tienen el derecho de conocer, entender de forma gratuita, sobre la persona que se va a hacer cargo de sus datos personales, también sobre la información y los pasos de cómo se puede acceder a ella, el encargado deberá establecer lo que son métodos flexibles y razonables para que el ejercicio de este derecho sea más fiable, este proceso se dará dentro del plazo de los 15 días.

2.2.1.3.3. Derecho de rectificación y actualización.

En este derecho la titular debe conocer su rectificación y a su actualización de los datos personales, sea que se encuentren intactos o incompletos, se deberá presentar su debido justificativo en el momento exacto, para poder adquirir tendrá un plazo de quince días, dentro de ese mismo plazo se deberá dar a conocer el destinatario, el caso de la rectificación o actualización que se solicita.

2.2.1.3.4. Derecho de eliminación.

La persona encargada de este tratamiento deberá implementar métodos más factibles para poder eliminar, para poder asegurar los datos personales. La o el titular de este derecho a de pedir lo encargado de todos sus datos que se haga de suprimir

siempre y cuando sean necesario, por ejemplo.

- Cuando el tratamiento no cumple con lo establecido en la ley.
- Cuando dicho tratamiento no sea útil para poder finalizar el cumplimiento.

- Que los datos personales ya hayan llegado a su finalidad del porque los fueron recogiendo.
- Cuando ya se venció lo que es el plazo de la conservación de los datos personales.
- Cuando el trámite llegue a afectar los derechos fundamentales ya sea de forma individual o colectiva.
- Cuando el consentimiento prestado o señalado revoque para uno o varios fines en específicos, sin justificación alguna.
- Cuando haya alguna responsabilidad legal.

2.2.1.3.5. Derecho de oposición.

La o el titular de este derecho puede negar o incluso oponer, sobre todos sus datos personales en tales como:

- No se afecten los derechos o incluso libertades de terceras personas, este tratamiento es ordenado por la ley.
- Cuando tengan por objeto lo que es la mercadotecnia directa.
- Cuando no sea necesario el consentimiento sobre un interés ilegitimo, siempre y cuando la ley no disponga lo contrario.

2.2.1.3.6. Derecho a la portabilidad.

La o el titular sobre los datos personales tienen derecho a poder obtener sus datos personales en un soporte informático donde esta se pueda guardar con más facilidad, también puede pedir el cambio de la persona responsable del tratamiento, es decir, este derecho nos da la posibilidad de recibir todos los datos personales para tenerlos guardados, también nos facilita transmitir nuestros datos a otro encargado responsable del dicho tratamiento, deberán facilitar el ejercicio de este derecho (Abogados, 2018)

Estos derechos también tienen una limitación en el tratamiento de los datos personales, como en este derecho no podrá ejercer un tercero sobre los datos personales, incluso cuando estos datos sean entregados al cliente o usuario del tratamiento por terceras personas.

2.2.1.4. Legalización vigente sobre el robo de identidad.

Como bien sabemos el mundo en el que vivimos es considerado como "la era digital", por su constante evolución ya sea en tiempo o en espacio, bien es cierto que la tecnología nos trae beneficios, pero también consecuencias y uno de ellos el robo de datos personales, es la forma de fraude donde una persona sustrae sus datos personales sin su consentimiento, con el fin de cometer delitos u obtener beneficios asiéndose pasar por la víctima, es decir, es como si un ladrón robara la identidad de otra persona y la explotara a su beneficio.

Dentro del robo de datos personales encontramos lo que son derecho, ahora bien, según CABANELLAS, nos manifiesta que el derecho es "colección de principios, preceptos y reglas a que están sometidos todos los hombres en cualquiera sociedad civil, para vivir conforme a justicia y paz; y a cuya observancia pueden ser compelidos por la fuerza" (Hernández Vera, 2019)

El Código Orgánico Integral Penal (COIP) establece estos delitos contra la intimidad, encontramos en el Articulo 212 nos habla sobre la suplantación o robo de datos personales o identidad, aquí la persona sin importarles la forma en la que llegue a suplantar la identidad de otra persona, para obtener un beneficio para un tercero o para sí mismo, actuando con mala fe, en perjuicio de una persona, deberá será sancionada con la pena privativa de libertad entre uno a tres años.

2.2.2. Procedimiento para una mejor seguridad cibernética.

La tecnología avanzando al pasar de los años, causando un gran impacto en la sociedad, trayendo sus beneficios como la comunicación, ayudas en el área de medicina, en el área de la ciencia, emprendimientos, entre otros, también sus consecuencias en este caso los ciber delitos o ciber delincuencia, vulnerando muchos derechos como a la intimidad, perjudicando la integridad incluso por medio de pornografías o secuestros.

2.2.2.1. Donde podemos denunciar los delitos de robo de datos personales.

Al momento de ser vulnerados o violentado algún derecho por los delincuentes cibernéticos como la identidad o los robos de datos, se podrá acercar a la fiscalía para dar a conocer la denuncia o incluso se podrán acercar a la Unidad de Investigación de Delitos Tecnológicos, como otra opción se podrán dar aviso al 1800-Delitos.

2.2.2.1.1. Fiscalía general del estado.

Basándonos en el "artículo 195 de la Constitución de la Republica del Ecuador", nos establece que la fiscalía se encargará de toda la investigación pre procesal y procesal penal, deberá ejercer dentro de la acción pública, basándose en el principio de oportunidad y por supuesto de la mínima intervención, teniendo en cuenta los derechos de las víctimas, de haber reunido todos los elementos de convicción se les acusará a los infractores frente a un juez competente, dando así su respectiva responsabilidad legal.

2.2.2.1.2. ¿Unidad de investigación de delitos tecnológicos?

Los encargados de las políticas y sobre todas directrices de estas investigaciones, Ministerio Publico y la Policía Judicial, estos juntos con un Coordinador Nacional, los Agentes fiscales y las demás partes de la Unidad que tengan conocimientos sobre los delitos informáticos.

Dentro de la tecnología de información podemos encontrar lo siguiente:

- Los diferentes tipos de lenguajes en la programación.
- Todo lo que tenga que ver con sistemas de operaciones y archivos.
- Los protocolos de comunicación.
- Los circuitos electrónicos.
- Y todo el esquema de computadores.

Dentro de la seguridad de datos podemos encontrar lo siguiente:

- El principio de seguridad informática.
- Las políticas y el procedimiento.
- Un análisis de la seguridad informática y sus vulneraciones.
- Un análisis de la administración de riesgo.
- La clasificación sobre la información.
- Los mecanismos y principios de la seguridad informática.

2.2.2.1.3. ¿El 1800-delitos?

El 1800-Delitos nace a partir del año 1999, en el 2008 fue aprobada por el presidente de la Republica del Ecuador, Rafael Correa por medio del Ministerio del Interior, este programa tiene una relación directa con la Policía Nacional, cumpliendo una responsabilidad en la ciudadanía con la seguridad, este servicio es confidencial, las personas que llegan a trabajar en este servicio, por seguridad no desean estar presentes en fotografías o en videos conferencias.

Para poder denunciar es necesario ir personalmente a la fiscalía o a la defensoría del pueblo, este es un programa encargado de recolectar información de diferentes tipos de delitos.

2.2.2.1.4. Pasos para denunciar un ciber delito.

Se deberá reunir evidencias contundentes.

Se deberá reunir todas las pruebas necesarias sobre el delito cibernético que se ha cometido, como pruebas documentales podemos encontrar las capturas de pantalla, los correos electrónicos, los registros de chat o páginas web y como otra opción puede ser los mensajes de texto.

La denuncia.

Al momento de saber que se cometió cualquier tipo de delito cibernético se trasladará a poner su respectiva denuncia acudiendo a las autoridades competentes como la Policía Nacionales especializados en estos delitos, en la fiscalía general se deberá poner esta denuncia con todas las pruebas ya recolectadas anteriormente.

El procedimiento.

Una vez aplicada la denuncia se deberá seguir las instrucciones que nos han brindado las autoridades, se dará cuidadosamente ya que dentro del procedimiento se podrá adquirir información adicional incluso llegar a participar en entrevistas.

La protección de cada dato personal.

Si se llega a comprobar que se ha violentado sus datos personales, se podrá presentar la denuncia a la Superintendencia de Protección de datos, se encargaran de tomar medidas necesarias y se tomara en cuenta la investigación correspondiente.

2.2.2.2. Que derechos tiene la victima durante el proceso de robo de datos personales.

Según lo establecido en la EcuCERT el robo de datos personales puede llegar a ocasionar problemas de credibilidad y también dañando o perjudicando la economía de cada víctima.

La Asamblea General de las Naciones Unidas en el año de 1985 el 29 de noviembre tiene su propia definición sobre las Victimas, nos establece que todas las personas ya sea natural o jurídica, sin importar la forma individual o colectiva, que hayan sufrido alguna vulneración incluso lesiones de forma, emocional, física, pérdidas financieras o que hayan violentado un derecho fundamental, por medio de una acción u omisión, como consecuencia llegando a violentar la legislación penal vigente, entre las victimas podemos incluir a los familiares o terceras personas.

2.2.2.2.1. Derecho a la protección.

Toda persona que llega hacer víctima de estos delitos cibernéticos tiene derecho a recibir protección cuando se presenten lo que son amenazas o incluso represarías, incluyendo lo que es la protección de la identidad y su integridad ya sea física o emocional.

2.2.2.2.2. Derecho a la denuncia.

Las victimas tiene la obligación de denuncia si se ha cometido un delito cibernético, esta denuncia se dará ante autoridades competentes, por ejemplo, la fiscalía general de procesos y la policía Nacional que son especializados en delitos cibernéticos.

2.2.2.2.3. Derecho a la información.

Las víctimas de estos delitos cibernéticos tienen derecho a ser informados de manera inmediata sobre su caso, todo lo que tiene que ver con los procedimientos legales y las medidas que van a tomar para resolver dicho problema,

2.2.2.2.4. Derecho a la asistencia.

Las víctimas de los delitos cibernéticos tienen derecho a una asesoría y sobre todo a la asistencia que se dé de forma legal dentro del sistema judicial.

El Código Orgánico Integral Penal (COIP), nos establece que la víctima se considera un sujeto procesal de igual manera la persona procesada, como las principales características encontramos a la fiscalía y a la defensa. El cuerpo legal ya entes mencionado llega a sancionar a los delitos informáticos se dan por los medios informáticos.

Art. 77. Nos establece sobre la reparación integral, que nos quiere decir esto, que esta reparación consiste en la dar una solución ya sea de manera objetiva o incluso simbólica, donde se pueda restituir el daño de la manera más posible, sobre la situación de los hechos fundados y llegue a satisfacer las necesidades a la víctima, llegando a poner un fin a las infracciones que se han cometido, recordemos que toda su naturaleza y su cuantía deberán depender del nivel de daño ocasionado al bien jurídico.

Art. 78. Dentro de los mecanismos de reparación no se pueden excluir formas de reparación de forma individual o incluso colectivas. Nos establece también sobre las indemnizaciones por daños inmateriales y daños materiales, refiriéndose así a la compensación por cualquier tipo de perjuicio que este derivado a una infracción penal, donde esta puede ser relevado de manera económica.

Los derechos se encuentran amparados en diversas normativas legales una de ellas es el Código Orgánico Integral Penal, la Constitución de la Republica del Ecuador, como también los tratados Internacionales de los Derechos Humanos, tomando en cuenta también los cuerpos legales como la Fiscalía, la Policía Nacional, estos cuerpos cuentan con una unidad de vigilancia especializada para los delitos cibernéticos.

Debemos recordar que los delitos cibernéticos o ciber delitos en la actualidad se ha presentado una mayor gravedad dentro de la sociedad, siendo su principal objetivo la población atacando a los grupos más vulnerables con el fin de estafar y obteniendo un beneficio económico.

2.2.2.3. Las obligaciones y responsabilidades legales de las instituciones en el proceso de robo de datos personales.

Las empresas o instituciones públicas deben tomar en cuenta como pueden proteger estos datos, antes de ser recabados, utilizados y por supuesto almacenados para así poder cumplir todos sus requisitos legales, dentro de la protección de datos para poder mantener la confianza de sus clientes, las instituciones juegan un rol de reputación y responsabilidades legales, es decir no solamente es "instalar un servicio" o "sistema seguro" se trata más de proteger todos los datos recabados, debemos recordar que muchas veces estos sistemas son vulnerados por los delincuentes cibernéticos.

2.2.2.3.1. Los datos personales.

1. Los nombres y apellidos.
2. El lugar, es decir, el domicilio.
3. La cedula de identidad o ciudadanía.
4. La dirección de los correos electrónicos.
5. Los números telefónicos.
6. La dirección de internet.
7. Los datos de emergencia, como hospital o médicos.

Toda la responsabilidad legal cae en manos de las instituciones ya sea públicas o privadas, basándose en el principio de protección proactiva de datos, debemos tener en cuenta también a los terceros involucrados como los proveedores y los accionistas.

En el mes de mayo del año 2023 entra en vigor lo que es las medidas correctivas y con ella las sanciones que establece la Ley de Protección de datos Personales, aprobado por

la Asamblea Nacional en el año 2021, dando así a las empresas Nacionales un año para poder regular y cambiar su proceso, creando así una identidad que es conocida como la Superintendencia de Protección de Datos.

Los funcionarios o servidores públicos, que hayan cometido una infracción leve que se encuentre tipificado en la ley puede ser por acción u omisión, se sancionara con una multa de uno a diez salarios básicos unificados del trabajador en sí. Los funcionarios o servidores públicos, que hayan cometido una infracción grave que se encuentre tipificado en la ley, ya sea por acción u omisión, se sancionara con una multa de diez a veinte salarios básicos unificados del trabajador en sí.

2.2.2.4. La protección de datos.

Se encuentra promulgada desde el año 2021 por la Ley Orgánica de Protección de Datos Personales, las instituciones tienen varias responsabilidades junto con ellas obligaciones para garantizar la seguridad y sobre todo la privacidad de su información:

- Consentimiento del titular.
- La seguridad de datos.
- El acceso y la rectificación.
- La suspensión y la oposición.
- La facilidad de portar sus datos,
- Las notificaciones de Brechas sobre la seguridad.
- La evaluación del impacto.
- Deberá ser transparente y responsable
- Deben ser capaz.
- Debe estar concientizado la o el titular.

Todas estas obligaciones ya mencionadas anteriormente son consideradas dentro de las instituciones que manejan todo lo que tiene que ver con datos personales de sus usuarios, se deberá de manejar de una manera responsable para así podrá proteger la privacidad, la integridad de cada usuario que confía en esta Institución.

2.2.3. La tecnología en los delitos cibernéticos.

2.2.3.1. Uso de la tecnología avanzada como malware o el phishing.

2.2.3.1.1. Los malware.

Es un sistema malicioso o también es conocido como un "código malicioso" "Software malicioso", fue diseñado para poder dañar, manipular o alterar cualquier sistema informático o cualquier usuario al azar donde se llegue a insertar en cualquier tipo de dispositivo, la mayor parte de ataques cibernéticos se dan por este código o software, adaptándose a si a cualquier tipo de programa, los ciber delincuentes adoptan al malware y es utilizado para diferentes actividades, bloqueando ya sea la computadora o el teclado, para poder pedir dinero como un supuesto rescate, este rescate usualmente se suele pagar con moneda Bitcoins.

- A los dispositivos de los usuarios mantener como rehenes, es decir, todos sus datos o redes incluso las bancas móviles las mantienen congeladas, para obtener un beneficio económico.
- Obtener lo que es un acceso protegido, es decir, no autorizado, como los datos o activos que son de vital confidencialidad.
- Es utilizado también para robar lo que son las credenciales como las tarjetas de créditos hasta información valiosa.
- Alteran también a los diferentes sistemas, bancos, instituciones gubernamentales.

Un dato muy importante en el año 2022 los malware son responsable del 17% de delitos en el Ecuador, usados con un fin malicioso como, infiltrarse en un sistema de información sin autorización alguna, se puede infiltrar en forma de:

- El Virus: El virus informático es un “código” o “programa malicioso” que sirve para modificar funcionamientos de un equipo, debemos tener en cuenta que el virus está diseñado para poder multiplicarse de un dispositivo a otro.

- Troyanos: En denominado como el caballo de troya, que es usado por los Malware y se camufla como un programa legítimo y sobre todo inofensivo, la mayoría de estos virus tienen la finalidad de controlar el equipo del usuario.

- El Ransomware: es parte de los Malware, el software, ese programa se da con el fin de extorsionar a las personas u organizaciones.

2.2.3.1.2. El phishing.

Phishing es un tipo de ataque cibernético, se da por medio de correos electrónicos, por medio de llamadas e incluso sitios web, dándole permiso a estos delincuentes a acceder a sus datos personales o llegando a descargar los malware, para así poder acceder a su información personal y cometer cualquier tipo de robo, con el fin de obtener un beneficio económicos ya sea de forma directa o por medio de terceras personas.

2.2.3.1.3. El banco pichincha (phishing).

Según el banco pichicha nos da a conocer que el phishing es un conjunto de herramientas informáticas que se utiliza como medio para poder suplantar la identidad por medio de canales falsos, también, se hacen pasar por empresas reconocida o incluso por personas comunes de sus posibles víctimas, asiéndose pasar como un ataque de ingeniería social.

Podemos decir que el Phishing es un tipo de ataque de Ingeniería Social, donde su objetivo en sí es incentivar que su posible victima acceda a lo que son sitios web inseguros, o incluso abrir archivos que parezca ser seguros y amigables como son las ofertas, los anuncio o incluso las notificaciones de los bancos, provocando así al usuario gran curiosidad, al momento de solo dar clic, ya le accede todos los permisos para poder acceder a su dispositivo y manejarlo a su antojo.

El phishing cuenta con diferentes sistemas o técnicas:

- La smishing.
- La vishing.
- El phishing en las redes sociales.

2.2.3.2. Inteligencia artificial (IA).

La inteligencia artificial anteriormente solo eran visiones al futuro, por decirlo así narraciones en cuentos ficticios, en la actualidad con el paso del tiempo hoy por hoy esta inteligencia ha ido mejorando y por supuesto evolucionando, esta inteligencia es parte de la rama informática diseñando la tecnología, implementando esta herramienta en un dispositivo electrónico con los conocimientos humanos, ahora bien, esta inteligencia artificial no trata de cambiar a la raza humana más bien mejorar y desarrollar capacidades y atribuciones, es decir, por medio de este logaritmo la (IA) podemos tener, conceptos, ideas e incluso razonamientos del propio humano.

Según la universidad de Michigan encontramos cuatro tipos de inteligencia artificial:

- Las maquinas creativas: Se podría decir que es una de las formas más básicas, bueno las maquinas reactivas no tienen capacidad de recordar o tomar decisiones, mucho menos de tener memoria o recuerdos.

- La memoria limitada: La memoria limitada es al contrario de las maquinas creativas, estas tienen la capacidad de almacenar información, esta información puede ser del pasado, se da me manera transitoria, es decir, tiene la capacidad de poder decidir o dar su punto de vista, pero con cosas del pasado.
- La teoría de la mente: Esta teoría es un poco más avanzada, donde puede tomar sus propias decisiones o tratar de emparejar con los pensamientos de los seres humanos.
- La autoconciencia: Se considera como la última etapa del ser humano, es decir, que tiene la capacidad de decidir por si mismo, ayudando con la ciencia y a la evolución del pensamiento en el ser humano.

A la inteligencia artificial también lo podemos relacionar con lo que usualmente se le denomina “El enfoque humano” y “El enfoque ideal”.

En el “enfoque humano” consiste en lo siguiente:

- En los sistemas que usualmente piensan como humanos.
- En el sistema que usualmente actúa como verdaderos seres humanos.

En el “enfoque ideal” deberá contar con los siguientes:

- Se dará el sistema que llega a actuar racionalmente.
- El sistema donde llega a pensar de forma racional.

2.2.3.3. La importancia de unos firewalls.

Como sabemos el firewall es un sistema que se encuentra una serie de reglas, se encarga de bloquear o también de autorizar cada sistema, código o virus que trata de incluirse en el dispositivo, es decir, se encarga de proteger lo que es nuestros dispositivos, de cualquier intimidación a diferentes instituciones o a cualquier persona en común, por este motivo

es muy importante implementar una firewalls en cada dispositivo que vayamos a utilizar, como nuestras cuentas bancarias, datos personales hasta llegar a tener información reservada.

El Banco Pichincha ha invertido e incrementado mucho en Firewalls como escudo de protección, para no ser vulnerados o manipulados los datos personales de sus usuarios, ahora bien, el firewall o también conocido como cortafuego, tiene la función de proteger los archivos de los equipos por medios de sitios web y eliminar cualquier tipo de malware (virus).

2.2.3.3.1. Defensa ante posibles hackers.

El firewall es un mecanismo de defensa entre el dispositivo electrónico y la navegación en el internet, muchas organizaciones y utilizan otros dispositivos donde que llegan a vulnerar el sistema, sin embargo, el firewall se encarga de controlar el tráfico de lo que entra y sale al dispositivo con mayor seguridad en la protección de datos.

2.2.3.3.2. Bloquea el acceso a los sitios web.

La Firewall permite detener y no dar paso a los posibles atacantes como Paginas o virus ya antes mencionado, las organizaciones aquí pueden crear medidas de defensa como escudos, para poder saber que páginas son confiables y no fantasmas.

2.2.3.3.3. Protege al usuario de códigos maliciosos.

El firewall se encarga de verificar todo lo que entra y sale del dispositivo, con el fin de verificar y captar a los virus, spam, gusanos o inclusos otros medio que lleguen a violentar las políticas de dichas empresas, organizaciones o negocios, llegando a si a vulnerar el sistema, este tipo de sistema se detecta esos ataques cibernéticos porque tiene una lista plantada de ellos.

2.2.3.4. El funcionamiento de la machine en la detección fraudulenta.

La machine se maneja por medio de algoritmo, datos históricos, donde se incrementa lo que es la detección fraudulentas y sobre todo genuinas, se incluye también lo que son registros de las transacciones financieras, y otros tipos de disposiciones para poder detectar estos patrones fraudulentos.

Por otra parte, la machine ya mencionado anteriormente puede adaptarse y entender estos indicadores que se hacen pasar desapercibidos para así comer cualquier tipo de fraude, este sistema se puede dar de dos formas:

- Puede ser supervisada: Se puede incrementar algoritmos para poder aprender de los datos, y para que pueda dar a conocer nuevos datos ya sea que estén etiquetados o no etiquetados.

- Como a su vez no puede ser supervisada: Aquí se incrementan los datos no etiquetados, esto nos ayuda para poder descubrir nuevos patrones y esto se maneja de forma independiente.

La detección fraudulenta junto con la machine se encargan de identificar lo que son las anomalías y las tácticas que no se han sido detectados con anterioridad por medio de estas acciones fraudulentos.

2.2.4. Delitos cibernéticos en el banco pichincha ecuador.

2.2.4.1. Medidas de protección del banco pichincha.

2.2.4.1.1. La ciberseguridad.

El objetivo de la ciberseguridad es nada más que proteger las aplicaciones, dispositivos informáticos, sobre todo los datos confidenciales y los financieros activos de las personas, sobre todo combatir con los virus informáticos ya anteriormente mencionados, estos

ataques son diseñados para poder manipular o dañar e infiltrarse en las empresas e instituciones, donde presentes sus servicios lícitos y sobre guarden los datos personales.

El avance de la inteligencia artificial se ha dado de forma negativa apoderándose de los delitos cibernéticos, las empresas de seguridad establecen que combaten a diario con estos delincuentes y se establece que en el año 2025 se estará pagando como seguridad alrededor de 10.5 billones de dólares, con el fin de disminuir estos ataques.

- Se ha dado a conocer que se es posible detectar cuando se sufre algún tipo de vulneración.
- La inteligencia artificial junto con los centros de procesamientos de datos ayuda a detectar cada día estos delitos.
- La inteligencia artificial ayuda también a detectar lo que son las identificaciones falsificadas y así proteger los datos de los demás usuarios.

2.2.4.1.2. La inteligencia artificial en finanzas.

Tenernos bien claro que todas las empresas deben brindar información a los usuarios de forma detalla, a pesa de tomar en cuenta todas estas medidas de seguridad muchas veces son afectados incluso por el factor humano, aquí es donde interviene la inteligencia artificial, para poder defender estes tipos de problemas, por medio de procesos y operaciones financieras.

- La inteligencia artificial nos ayuda reduciendo tiempo y sobre todo costos de forma automática.
- Nos ayuda a predecir aprendizajes de forma automática.

2.2.4.1.3. Consecuencias legales a las instituciones sobre el robo de datos personales.

Para llegar a suplantar una identidad o extraer datos personales actuando con mala fe uno de los datos más utilizados donde cometen estos delitos en la Spam esto consiste en lo llamado “publicidad” enviando una cantidad de mensajes a sus posibles víctimas.

La Agencia de Regulación y Control de las Telecomunicaciones la (Arcotel) recomienda tomar medidas serias para poder evitar estos tipos de conflictos y reducir el riesgo de ser suplantado su identidad o de ser extraído sus datos con fines maliciosos:

- Prevenir y no dejar ya sean copias o documentos de identidad.
- Tener conocimiento sobre lo que la suplantación de identidad sobre las aplicaciones más usadas por ejemplo el phishing u otras aplicaciones.
- Configurar lo que es la privacidad y la seguridad en los medios electrónicos que utilicemos.
- Utilizar las medidas de seguridad, como cambiar de contraseñas cada cierto tiempo.
- No ingresando datos en páginas sospechosas, por hacer una compra en la web.
- Publicar datos personales en las redes sociales.
- Es recomendable usar el doble de autenticación en las aplicaciones que los permita.

Las personas jurídicas pueden llegar a ser multadas hasta con el 1% de su facturación por hacer mal uso de los datos personales de sus clientes o usuarios. Las multas y otras sanciones administrativas entraron en vigor desde el 26 de mayo de 2023, a dos años de la publicación de la Ley de Protección de Datos Personales. Sin embargo, aún no está creada la Superintendencia de Protección de Datos Personales, entidad que debe velar por el cumplimiento de la norma ya establecida que estará a cargo de imponer las sanciones correspondientes (González, 2023).

Una de las obligaciones que establece la Ley de Protección de Datos es que las empresas deben contar con su consentimiento de manera libre e informado de las personas para hacer uso de sus datos personales (González, 2023)

Como ya habíamos mencionado en un capítulo anterior, los titulares deben informar el tratamiento que se les va a dar sobre sus datos personales, en caso de las empresas deberán respaldar como llegaron a obtener esos datos. En los últimos dos años han implementado medidas de seguridad para respaldar a la ley y sobre todos a su información personal como:

- Implementando políticas de protección de los datos.
- Capacitando al personal encargado de gestionar los datos.
- Implementando medidas técnicas de seguridad para evitar cualquier tipo de riesgo o vulneración.
- Estableciendo clausulas.
- Asignando también un delegado para la protección de estos datos, es obligatorio.

Tipos de infracciones La Ley de Protección de Datos Personales determina la infracción leve, esta puede llegar a tener una multa hasta el 0,7% de la facturación de una empresa. Algunas infracciones de este tipo son:

- No tramitar las peticiones o quejas de los propietarios de los datos o hacerlo fuera de tiempo.
- Mantener políticas de protección de datos personales diferentes al tratamiento que se les está dando a los datos.
- Se deberá elegir a una persona para estar a cargo del tratamiento de datos personales de cada usuario que no ofrezca garantías suficientes.
- El encargado puede ser un proveedor de servicios de mercadeo.

Por una infracción grave, una compañía puede ser multada con hasta el 1% de su facturación, entre las consideradas como graves estarían:

- Utilizar información para fines diferentes a los que se informó al usuario.
- No podrá acceder o incluso comunicar a terceros sobre los datos personales sin haber cumplido los requisitos y los procedimientos que están establecidos en la ley.
- No implementar medidas para prevenir riesgos y vulneraciones a la seguridad de datos personales que hayan sido identificados.
- No notificar las vulneraciones sobre la seguridad a la Superintendencia de Protección de Datos y a sus titulares, cuando se dé una vulneración a los derechos fundamentales.

En el momento en el que no designe a un delegado para la protección de los datos personales cuando corresponda, la Superintendencia también podrá sancionar con las medidas correctivas, como el cese de tratamiento de los datos, en este caso la eliminación de los datos o la implementación de medidas ya sea técnicas o incluso jurídicas para un adecuado uso de los datos (González, 2023).

2.2.4.2. Aumento de los ataques cibernéticos en el banco pichincha, ecuador año 2021.

2.2.4.2.1. Correos fraudulentos en el banco pichincha.

El 18 de febrero del año 2021 el Banco Pichincha dio a conocer sobre un “acceso no autorizado” por medio de correos electrónicos conocido como “pichincha Miles” sin embargo, no hubo daños a ningún recurso financiero de los usuarios del banco pichincha, cabe más recalcar que el banco pichincha dentro de sus políticas no están autorizados de

pedir cosas sencillas como números de tarjeta o incluso clave ya que son propios del usuario y deben ser protegidos.

Esta entidad financiera se encuentra cada día trabajando y velando por la seguridad y el manejo de los datos por parte de todos los proveedores, con el fin de prevenir este tipo de situaciones, la entidad también reconoce la preocupación de cada uno de los usuarios, garantizando protección absoluta de sus datos personales ya que su información hubiese sido sobre expuesta dañando y perjudicando a cada proveedor.

El 10 de octubre del año 2021 el Banco Pichincha tubo un error en el sistema, este sitio web se encontraba fuera de servicio por varias horas, después de unas 72 horas la entidad financiera por medio de su página oficial de Twitter dio a conocer que hay un "incidente de ciberseguridad" sin embargo, en banco pichincha se encontraba protegiendo los datos de los usuarios, afirmo que no hubo afectaciones ni vulneraciones a ningún banco financiero, dentro del sistema todos los usuarios y todos sus datos se pudo mantener bajo control, los bancos, los cajeros para hacer retiros o depósitos se encuentran operando con total normalidad incluso la banca móvil en cualquier dispositivo de cada usuario se encuentra protegido bajos las políticas del Banco Pichincha.

2.2.3.1. La superintendencia de bancos le exige al banco pichincha que tenga una auditoria forense propia.

En el año 2021 del mes de octubre el miércoles 20 la Sra. Ruth Aguirre de ese entonces encargada de la superintendencia se presentó ante la Comisión de desarrollo económico de la asamblea esta reunión se llevó a cabo para tratar del tema de inhabilitación en los sistemas "ataque cibernético" ocurridos en la semana del 8 y 9 por parte del banco pichincha, se tomaron barrios puntos en consideración para mejorar el sistema de la entidad financiera como poner una auditoria forense, para poder determinar las fallas y

de donde se originó, sin embargo, esta auditoria debe ser propia solo para el equipo informático y así poder determinar desde la raíz cual es el problema.

2.2.3.1.1. Auditoria forense en el ecuador.

Podemos conocer que auditoria forense es en si un proceso que se encarga de revisar y analizar todo lo relacionado con los registros financieros, esto lo hace de forma detallada, se hace con el finde poder evitar irregularidades financieras como el fraude o ataques cibernéticos, teniendo así un respaldo seguro y confiable para las respectivas responsabilidades legales por parte de los infractores, se debe tener en cuenta que no cualquier persona puede ser encargada de tal responsabilidad, debe ser una persona capaz y altamente profesional con tal experiencia de poder identificar los fraudes y contando también con experiencia en leyes.

2.2.4.1. Aumento de ciberataques en el estado ecuatoriano.

La superintendente de Bancos la Sra. Ruth Aguirre dio a conocer que a mediados de la pandemia del COVID 19 que se dio en el año 2019 donde se implementó los servicios digitales, hasta entonces aumentado los ataques de delitos cibernéticos multiplicándose por cuatro, esto durante los últimos dos años, durante la pandemia los servicios por parte del Banco Pichincha estuvieron funcionado con normalidad por tal motivo se tuvo que dar atención remota, durante el año 2019 y 2020 y tomando en cuenta los servicios digitales y remotos las transacciones virtuales se incrementó un 33%, así también se tomó en cuenta gestionar más seguido la seguridad de la información.

Además, la superintendente la Sra. Aguirre dio a conocer se dio un seguimiento supervisando los controles de forma integral y sobre todo focalizada, dando una clara observación a la infraestructura de las transacciones y la banca electrónica, esto se tomó

en consideración desde el año 2019, en el año 2020 la superintendencia también hizo una revisión sobre los riesgos de crédito y liquidez.

La superintendencia de bancos realizo la revisión sobre el plan de continuidad y de estabilización tecnológica, esto es importante ya que se considera un requisito importante para todos los bancos que se encuentra en el Ecuador. Por segunda vez la superintendente invita a su representante del Banco Pichincha, pero no acudió, sin embargo, se hizo presente con un correo electrónico diciendo que es una entidad financiera privado, también dio a conocer que las atribuciones de control, supervisión y vigilancia ya fueron ejercidas por la Superintendencia, actualmente el Banco Pichincha se encuentra atendiendo los diferentes requerimientos, garantizando así su cumplimiento sobre marco perteneciente encargado del regular.

2.3. Marco legal.

En la presente investigación análisis del derecho a la privacidad, en base a los datos personales, en delitos cibernéticos, banco pichincha, año 2019, las siguientes normativas que se encuentran amparados en el estudio de la presente investigación, se realiza en el siguiente marco legal, por medio de leyes, normas, reglamentos, doctrina, jurisprudencia.

2.3.1. Constitución de la república del ecuador (C.R.E)

COMUNICACIÓN E INFORMACIÓN.

- En el Art 16, numeral 2 y 3.
  2. “El acceso universal a las tecnologías de información y comunicación”.
  3. “La creación de medios de comunicación social y al acceso en igualdad de condiciones al uso de las frecuencias, de espectro radioelectrónico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas

libres para la explotación de redes inalámbricas" (Constitución de la Republica del Ecuador, 2011, 13 de julio)

Tanto el acceso a la información es crucial, también se da por igualdad el acceso a los medios de comunicación ya que es un componente esencial para la sociedad ya que las autoridades deben manejar de forma proactiva y sobre todo implementar políticas para la equidad de estos ámbitos.

DERECHOS DE LIBERTAD.

- Art 66 numeral 20 y 21

20. "El derecho a la intimidad personal y familiar".

21. "El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; esta no podrá ser retenidas, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial, y con la obligación de guardar el secreto y de los asuntos ajenos que motiven su examen, este derecho protege cualquier otro tipo o forma de comunicación" (Constitución de la Republica del Ecuador, 2011.p.31).

El derecho a la intimidad ya sea de forma personal o familiar asi también como la inviolabilidad de los datos personales, ya que es un pilar fundamental para la sociedad, para poder respetar, proteger la integridad y la dignidad de cada persona.

DERECHOS DE PROTECCIÓN.

Art 76.- - "En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas".

1. "Corresponde a toda autoridad administrativa o judicial, garantizar el cumplimiento de las normas y los derechos de las partes".

2.3.2. Código orgánico integral penal. (COIP)

El art 190.- "La apropiación fraudulenta por medio electrónicos. La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años" (Código Orgánico Integral Penal, 2021.p.75).

- El art 191.- "Programación o modificación de información de equipos terminales móviles. La persona que programe o modifique la información de identificación de los equipos terminales móviles, será sancionado con una pena privativa de libertad de uno a tres años" (Código Orgánico Integral Penal, 2021.p.75).
- El art 195.- "Infra estructura ilícita. La persona que posee infraestructuras, equipos, base de datos o etiquetas que permitan programar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionado con una pena privativa de libertad de uno a tres años" (Código Orgánico Integral Penal, 2021.p.75).

En el artículo 190; 191 y 195 nos establece una base legal y factible sobre la apropiación fraudulenta por los medios electrónicos relacionados con el presente trabajo sobre el robo de datos personales en el banco pichincha, es decir, define claramente el delito por el cual tiene su responsabilidad legal y que bienes jurídicos se llegan a vulnerar, en casos de que sean modificadas o alteradas con el beneficio de un tercero para poder tener un fin económico, el COIP es encargado de sancionar estas conductas.

2.3.3. Ley de protección de datos personales.

DERECHOS.

Art. 13.-Derecho de acceso. –"El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales

y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna. El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho, el cual deberá ser atendido dentro del plazo de quince (15) días" (Ley de Protección de Datos Personales, 2021.p.12).

Art. 14.- "Derecho de rectificación y actualización. -El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos" (Ley de Protección de Datos Personales, 2021.p.12).

- Art. 15.-Derecho de eliminación. – "El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales, cuando":

1) El tratamiento no cumpla con los principios establecidos en la presente ley.

2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;

3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados.

4) Haya vencido el plazo de conservación de los datos personales.

5) El tratamiento afecte derechos fundamentales o libertades individuales.

6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o, 7) Exista obligación legal (Ley de Protección de Datos Personales, 2021.p.12).

Art. 18.- "Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. -Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad" (Ley de Protección de Datos Personales, 2021.p.13).

Art. 22.-Derecho de consulta. – "Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, de

conformidad con la presente Ley" (Ley de Protección de Datos Personales, 2021.p.15).

Todos los articulos mensionados anteriormente que se encuetra establecido en la Lay Organica de Protección de Datos Personales, nos hablan de los derechos que tienes los usuarios del Banco Pichincha sobre sus datos perosonales, de ser comunicados en casos que sean victimas de estos delitos, conocer quienes van a ser sus represntantes legales, tener derecho a sus consultas y ser correspondidos de una forma amigable y entendible, también como usuario es importante saber a que entidad juridica confimos nuestros datos y saber como se encuentra valorado su sistema de seguridad.

2.3.4. Acuerdo ministerial.

"Acuerdo Ministerial N°6, publicado en el Registro Oficial Suplemento 479 del 23 de junio del 2021, se publicó la Política Nacional de Ciberseguridad que tiene como objetivo en su Art 2".

Ar 2.- "El objetivo de la presente política es construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población, y la protección de los bienes jurídicos, del estado en el ciber-espacio".

CAPITULO III: MARCO METODOLÓGICO.

3.1. Metodología.

En la presente investigación en base al análisis del derecho a la privacidad, en base a los datos personales, en delitos cibernéticos, banco pichincha, año 2019, teniendo así un análisis preciso sobre este tema, se aplicó la metodología cualitativa, este método consiste en investigar diferentes estrategias como, la recopilación y análisis de datos pero no numéricos, este método se enfocó más por medio de la comunicación, en entrevista, es decir, se basa más en el procedimiento lógico dentro de la sociedad o de forma individual,

para poder comprender diferentes tipos de conceptos, experiencias, las emociones e incluso los comportamiento y también las opiniones que nos contribuyan las diferentes persona, sobre el tema ya mencionado anteriormente.

3.2. Tipo de investigación.

El tipo de investigación que se utilizo es descriptivo, es un método para poder recolectar información, para poder demostrar la relación que se describe con el tema, se dio también la investigación explicativa, esto nos da a conocer que tiene una relación causal, es decir, se describe o se acerca al problema ya planteado, trata de precisar la casusa del mismo, por otro punto tenemos la estructura objetiva y subjetiva, en relación con el tema, los objetivos, la hipótesis, el marco metodológico y sobre todo el problema sobre el análisis del derecho a la privacidad, en base a los datos personales, en delitos cibernéticos, banco pichincha, año 2019.

3.3. Técnica e instrumentos de investigación.

El método que se aplico es el método cualitativo, nos basamos en:

- En diferentes tipos de encuestas y sobre todo la recopilación de datos a los estudiantes de la Universidad Estatal de Bolívar de la facultad de Jurisprudencia, Ciencias Sociales, a los docentes especializados en el área de penal, a los representantes de la Institución financiera y al Ingeniero en Software especializado en sistemas.
- Se dio el análisis cualitativo, es decir, se dará el análisis de diferentes documentos, textos, doctrinas, y por supuesto leyes, normas, reglamento, jurisprudencia en sí.
- También encontramos las biografías, las fuentes confiables, las citaciones, la observación de participante desde sus experiencias o puntos de vistas.

3.4.Criterio de inclusión y criterio de exclusión.

Los criterios que se pudo llegar a recolectar, es el dialogo con las personas que lleguen a tener una experiencia directa, es decir, estos criterios podemos encontrar con los profesionales en el área del derecho, con los trabajadores del Banco Pichincha, con los Policías Nacionales, con los fiscales, con los Ingenieros en Sistemas, o en áreas relacionados con la criminología.

3.5.Población y muestra.

En esta investigación se encuentra directamente relacionado con el análisis del derecho a la privacidad, en base a los datos personales, en delitos cibernéticos, banco pichincha, año 2019, como población se dio a conocer a los estudiantes de la carrera de derecho, a los docentes especializados, en estas áreas lo podemos encontrar en la prestigiosa Universidad Estatal de Bolívar (UEB), sobre todo a los Ingenieros en sistemas y a los representantes del banco pichincha del cantón Caluma y el cantón Guaranda, esta información se presentará con su respectivo análisis en donde se encuentra centrado el respectivo problema.

3.6. Localización geográfica del estudio.

La investigación se aplicó a la población en general, a los encargados del Banco Pichincha, a los docentes especializados en el área de penal de la prestigiosa Universidad Estatal de Bolívar, también se aplicó a un Ingeniero especializado en sistemas de la provincia del Guayas.

3.7.Preguntas de la encuesta y sus importancias.

1. ¿Conoce usted sobre los ciberdelitos y que sugerencia nos daría?

Podemos conocer desde el punto de vista de los usuarios como de la población, teniendo en cuenta un porcentaje de conocimiento sobre los delitos cibernéticos si nos pueden dar

sugerencias desde el punto de vista ya sea porque han sido víctimas o por si algún motivo ha escuchado sobre este delito.

2. ¿Usted como usuario del Banco Pichincha ha sido víctima del ciberdelito?

Esta pregunta se le hace con la finalidad de saber si han sido víctimas o no de sus datos personajes dentro del Banco Pichincha.

3. ¿Le consta a usted que el Banco Pichincha tiene una seguridad adecuada a sus datos personales?

No podemos saber a profundidad ya que el Banco Pichincha tiene muchas medidas de seguridad, pero si podemos tener diferentes puntos de vista de cada profesional y las sugerencias que nos podrían dar.

4. ¿Cree usted tener garantías como usuario que sus datos personales están protegidos por el Banco Pichincha?

Esta es una pregunta muy común para saber que tanto conocimiento tienen de lo que firman o de lo que acceden, ya que al momento de ser usuarios del Banco Pichincha les dan a conocer cómo se rigen, que derechos tienen y a qué acceso puede hacer uso esta entidad.

5. ¿Conoce usted que los artículos 190 y 191 del Código Orgánico Integral Penal (COIP) se encarga de sancionar estos delitos cibernéticos?

Pues bien es cierto el Código Orgánico Integral Penal (COIP) se encarga de regular este tipo de conductas inapropiadas, la formulación de esta pregunta como de muchas tiene el objetivo de saber mas sobre estas sanciones y como podemos prevenirlas.

CAPITULO IV: RESULTADOS Y DISCUSIÒN.

4.1. Resultados.

4.1.1. Transcripción de entrevistas.

Por parte del Dr. Marco Vinicio Chávez Taco, docente de la prestigiosa Universidad Estatal de Bolívar, especializado en el área de Derecho Penal.

¿Conoce usted sobre los ciberdelitos y que sugerencia nos daría?

Si bien es cierto, las conductas relacionadas con el delito informático, tiene sus genes en la ley comercio y firmas electrónicas, no como una normativa sancionadora, sino como un antecedente a la protección de datos a través de medios informáticos, ahora bien, el Código Orgánico Integral Penal (COIP) ha implementado en armonía con el progreso informático, aquellas conductas que se adecuan a tipos penales relacionados con el tipo penal informático y que atentan al bien jurídico como las propiedades, la normativa que sanciona existe pero nuestro sistema adjetivo penal adolece de un verdadero sistema de investigación penal respecto de informática en lo que puede llevar en muchos de los casos a una impunidad, el derecho se transforma en base a las necesidades de la sociedad y como en la actualidad, existen transacciones financieras que se dan a diario, la ley cumple con la tipificación de estos delitos cibernéticos, pero también es responsabilidad de las instituciones que manejan datos subjetivos y es necesario contar con las respectivas seguridades ya que en muchos casos adolecen del sistema financiero.

¿Usted como usuario del Banco Pichincha ha sido víctima del ciberdelito?

No, yo no he sido víctima.

¿Le consta a usted que el Banco Pichincha tiene una seguridad adecuada a sus datos personales?

No me consta, pero si sería necesario que todas las Instituciones financieras cuente con un sistema de seguridad informática para garantizar los derechos de los usuarios.

¿Cree usted tener garantías como usuario que sus datos personales están protegidos por el Banco Pichincha?

Desconozco si el Banco Pichincha cuenta con el respectivo sistema de seguridad financiero.

¿Conoce usted que los artículos 190 y 191 del Código Orgánico Integral Penal se encarga de sancionar estos delitos cibernéticos?

Si, el Código Orgánico Integral Penal (COIP) los diferentes delitos informáticos como por ejemplo el acceso no consentido a sistemas informáticos y consecuente la protección de datos personales, el Código Orgánico Integral Penal si sanciona este tipo de conductas penalmente relevantes relacionados con los delitos cibernéticos.

Por parte del MSc. Ingeniero en software especializado en sistemas el Sr. Carlos Alexander Caba Satama.

¿Conoce usted sobre los ciberdelitos y que sugerencia nos daría?

Directamente como usuario no me consta como tratan los datos personales ya que definitivamente debería estar ligado a una entidad de regulación artículos incluso dentro de leyes que asegura que nuestros datos están de una manera respaldada de manera segura y confiable, respetando su integridad, fiabilidad y seguridad por supuesto, a medida que nosotros hacemos a los servicios del banco pichincha, por supuesto hay las políticas que nosotros mismo aceptamos ya sea en las aplicaciones móviles que se han vuelto muy famosas como la banca móvil o el pago de una, pues al momento que nosotros la utilizamos aceptamos las políticas y si nosotros nos tomamos el tiempo ahí se enlista todo de cómo se trata a que tenemos derecho y que nos respalda de nuestros datos personales, también en un poquito de información de que nosotros debemos hacerlo, yo debo conocer

y preocuparme de cómo se encargan de respaldar nuestros datos personales, entonces es una forma de preocupación mía.

¿Usted como usuario del Banco Pichincha ha sido víctima del ciberdelito?

No, afortunadamente no he sido víctima, pero si escuchado muchas veces podemos llegar a ser víctimas no directamente por alguna vulnerabilidad en el sistema del banco pichincha, también puede ser por ingeniería social, también puede ser por los famosos phishing que llegan a nuestros correos electrónicos que básicamente es el tratar de dar publicidad de un servicio que parezca del banco pichincha y trata de robarnos nuestros datos, incrustar virus, malware y demás, entonces no he sido víctima pero sé que es algo muy preocupante que si ocurre.

¿Le consta a usted que el Banco Pichincha tiene una seguridad adecuada a sus datos personales?

Claro por supuesto, como Ingeniero Informático y alumno de la maestría en ciberseguridad tengo conocimiento sobre los ciberdelitos que no es más que ataques. intentos de suplantación de identidad, robo de datos personales, en plataformas personales, es decir, a partir de herramientas informáticas, eso hace la referencia de ciber-delito, orientado al campo del tecnología y bueno, como sugerencia podemos decir que la vulnerabilidades y las amenazas pueden estar orientadas a muchos factores, al factor organizacional, a las políticas que plantea la organización, puede estar también las configuraciones en el software, a los equipos, la calidad de los equipos del software que se compra, también incluso a errores humanos como el propio trabajado, la ingeniería social que se puede aplicar en ello incluso muchas veces el atacante puede estar dentro de la empresa, entonces, las sugerencias van enfocados a todos esos puntos, reforzar las políticas, hacer firmar carta de compromiso a los trabajadores por diferentes

circunstancias, tener capacitadores y orientados al usuario en ingeniería social tener mucho cuidado de estar enfocados en canales de comunicación confiables, estar enfocados también la información confiable ´propia de la entidad bancaria, en este caso el banco pichincha porque son blancos muy fáciles por medios de comunicación y de más una arma en contra del propio usuario.

¿Cree usted tener garantías como usuario que sus datos personales están protegidos por el Banco Pichincha?

Una entidad bancaria como el banco pichincha está bajo varias entidades de regulación tanto nacionales como internacionales entonces, tanto la operatividad de ellos está en el cumplimiento de esa norma y bueno en primer instancia es una de las primeras, bueno yo como estudiante y profesional en algo las conozco y las e tratado entonces yo sé que una entidad para estar en funcionamiento debe cumplir además de conocimiento, como se tratan los datos, las típicas políticas "acepta usted las políticas de su uso y protección de datos" o también información que dice "el formulario que usted envía para el banco pichicha será utilizado para diferentes tratamientos " de una u otra forma nos está informando , si nos están dando esa garantía, ya que al momento de que nosotros hacemos uso de esos servicios nosotros aceptamos las obligaciones a cumplir y también derechos que tenemos como usuario.

¿Conoce usted que los artículos 190 y 191 del Código Orgánico Integral Penal se encarga de sancionar estos delitos cibernéticos?

Sí, estoy de acuerdo que estos artículos junto con otros anexos nos ayudan a saber que estos actos pueden ser castigados de la misma manera relacionados con el ciberdelito, como dije anteriormente tiene que ver con todo intento de ataque a una infraestructura

que no se está autorizado ya sea a obtener datos personales, información y muchas cosas más de ese tipo.

Por parte del Abogado Daniel Herrera Lara profesional en el área de derecho y usuario del Banco Pichincha.

¿Conoce usted sobre los ciberdelitos y que sugerencia nos daría?

Bueno, en si como ahora se abre una amplia gama en el tema de comisión de delitos cibernéticos que nuestro Código Orgánico Integral Penal ha ido teniendo un avance progresivo al momento de sancionar estas conductas punibles, pues la sugerencia que yo podría aportar es que siempre nosotros como usuarios utilizar cualquier tipo de servicios de banca, especialmente incluso por temas de tiempo y facilidad en nuestros dispositivos celulares, la sugerencia o recomendación que yo pudiera dar a cualquier usuarios es que siempre tratemos de ser cautelosos en la información que nosotros brindamos a través de las aplicaciones que notros tenemos descargados en nuestros teléfonos celulares.

¿Usted como usuario del Banco Pichincha ha sido víctima del ciberdelito?

No, eso no me ha pasado, pero si he oído en otros casos.

¿Le consta a usted que el Banco Pichincha tiene una seguridad adecuada a sus datos personales?

Bueno, yo no podría brindarle mucha información porque bien es cierto cuando uno accede a formar parte del banco pichincha o de otras Instituciones más, siempre a todos los usuarios se nos hace que aceptemos de forma previa y consintamos el manejo de nuestros datos personales para poder acceder aquellos servicios, entonces más que una garantía para mi yo creo que están administrados mis datos personales, no con seguridad, pero me rectificaría y presumo que sí.

¿Cree usted tener garantías como usuario que sus datos personales están protegidos por el Banco Pichincha?

Yo presumiría que sí.

¿Conoce usted que los artículos 190 y 191 del Código Orgánico Integral Penal se encarga de sancionar estos delitos cibernéticos?

A profundidad no los he analizados, pero si los he revisado.

Tabla 1: análisis de las respuestas en entrevista

PREGUNTAS	Marco Chavèz.	Carlos Caba.	Daniel Herrera.
¿Conoce usted sobre los ciberdelitos y que sugerencia nos daría?	Nos da a conocer un punto de vista muy amplia desde la tecnología que ha avanzado hasta la legislación ecuatoriana que se encarga de sancionar estos delitos.	No conoce los delitos cibernéticos, pero desde el punto de vista de ser usuario, pero del punto de vista profesional si lo conoce.	Los delitos cibernéticos han aumentado al igual que el COIP se encarga de sancionar estos delitos y en muchos casos se dan por el error propio del ser humano
¿Usted como usuario del Banco Pichincha ha sido víctima del ciberdelito?	No ha sido víctima de delitos cibernéticos.	No ha sido víctima de delitos cibernéticos	No ha sido víctima de delitos cibernético
¿Le consta a usted que el Banco Pichincha tiene una seguridad	Como usuario del Banco Pichincha no le consta que tienen una	Si, se mantiene al tanto ya que se encuentra relacionado en esta area y con los tipos	

adecuada a sus datos personales?	seguridad adecuada.	de ataques cibernéticos.	
¿Cree usted tener garantías como usuario que sus datos personales están protegidos por el Banco Pichincha?	Tiene conocimiento que el banco Pichincha tiene una seguridad algo adecuada, pero no al cien por ciento, sin embargo, si da sugerencias para poder mejorar la protección de estos datos.	Si, ya que al momento de acceder a nuestros datos al Banco y ser usuarios de esta, estamos al tanto de los reglamentos que se rigen esta entidad.	Si cree tener garantías de que sus datos personales están protegidos.
¿Conoce usted que los artículos 190 y 191 del Código Orgánico Integral Penal se encarga de sancionar estos delitos cibernéticos?	Como profesional en área de derecho penal tiene conocimiento de que estos artículos se encargan de regular estas conductas maliciosas.	Si conoce sobre estos artículos y que se encuentran vinculados otras leyes o reglamentos para poder sancionar estas conductas maliciosas.	Si tiene conocimiento, pero no lo analizado a profundidad.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES.

5.1.Conclusiones.

En el presente trabajo de investigación hemos aprendido mucho sobre los delitos cibernéticos, como llegan a operar estos delincuentes ya sea de forma grupal o individual y las responsabilidades legales, recordemos que en el ecuador estos delitos cibernéticos se encuentran tipificado en el Código Orgánico Integral Penal (COIP), en muchos casos estos delitos se dan por la falta de implementación de seguridad en las empresas o el descuido de uno mismo sobre sus datos personales.

Como ya sabemos los delitos cibernéticos pueden ocurrir en cualquier momento desde cualquier lugar del mundo, por medio de un dispositivo electrónico y un poco de información cibernética, la tecnología o "era digital" es muy importante hoy en día ya que estos delincuentes operan con diferentes tipos de programas "virus" como la Malware, el Phishing y sobre todo la inteligencia artificial "IA".

Debemos tener en cuenta que cualquier usuario puede ser víctima de estos ciberdelitos junto con ello los derechos que se vulneran cuando somos víctimas, se encuentran establecidos en los cuerpos legales como en el Código Orgánico Integral Penal (COIP), en la Constitución de la República del Ecuador (CRE), la Ley de Protección de Datos Personales y otras normativas, se puede considerar que los derechos violentados es la seguridad jurídica, la privacidad personal o familiar y los datos personales.

Por medio de la investigación que me he planteado sobre el análisis del derecho a la privacidad, en delitos cibernéticos en el cantón Guaranda, año 2020, se demostró que existe más vulneraciones de derechos por medio de los ciberdelincuentes en el cantón Guayaquil que en el cantón Guaranda, por su gran demanda en las empresas e incluso en la población mismo, habiendo más movimiento y mayor número de denuncias.

5.2. Recomendaciones.

Podemos dar puntos de vista en las Instituciones jurídicas, que implemente más estrategias en su rango de seguridad cibernética, ya que en muchas ocasiones es muy débil y cualquier persona o grupo de personas puede acceder a ella, como un permiso no autorizado.

Debemos tener en cuenta que cualquier persona puede ser víctima de estos delitos, por lo tanto, los ciudadanos deberíamos implementar estrategias de seguridad más seguido, ya sea en nuestros dispositivos electrónicos o donde tengamos información importante y también pedir una buena seguridad a las Instituciones financieras que están encargadas de nuestros datos personales.

Es importante dar a conocer a las autoridades competentes si hemos sido víctimas de estos delitos para que se puedan tomar medidas adecuadas, sabiendo que esto ya se encuentra tipificado en nuestra legislación ecuatoriana.

Que se implemente y se tenga más en consideración sobre los temas de delitos cibernéticos en las instituciones o ramas que tengan relación con la información informática, no importa si estamos en cualquier Provincia, Ciudad, Cantón o Parroquia, la seguridad cibernética se ha vuelto muy vulnerable y siendo así más factible acceder a nuestros datos donde los delincuentes llegan a utilizar diferentes estrategias, es recomendable denunciar y evitar uno mismo ser víctima de estos delitos cibernéticos.

Fotografías de las encuestas

BIBLIOGRAFÍA.

Ajila Pintado, A. G. (2020). Análisis jurídico de las leyes que amparan a víctimas del delito informático en Santo Domingo. DSpace de Uniandes: Análisis jurídico de las leyes que amparan a víctimas del delito informático en Santo Domingo

Campos, N. J. O. (2019). Normativa legal sobre delitos informáticos en Ecuador. *Revista Científica Hallazgos21*, *4*(1), 100-111. Normativa Legal sobre Delitos Informáticos en Ecuador - Dialnet (unirioja.es)

Carrasco, J. G. D. P., Salazar, S. J. L., & Paucar, C. E. P. (2024). Programa de prevención de ciberdelitos en instituciones educativas de Ecuador. *Revista Conrado*, *20*(96), 675-686. aitorres,+Gestor_a+de+la+revista,+A68 (1).pdf.

Centeno Aulla, H. D. (2024). Desarrollo de un módulo de seguridad basado en OSSTMM y OWASP para mitigar y controlar la seguridad en aplicaciones web caso de estudio: Sistema Médico Escuela Superior Politécnica de Chimborazo. DSpace ESPOCH.: Desarrollo de un módulo de seguridad basado en OSSTMM y OWASP para mitigar y controlar la seguridad en aplicaciones web caso de estudio: Sistema Médico Escuela Superior Politécnica de Chimborazo.

¿Cuáles son las infracciones a la Ley de Datos Personales? (primicias.ec)

Lucero Burbano, J. L. (2023). *Delitos informáticos y la violación de los derechos constitucionales de integridad e intimidad* (Doctoral dissertation, Pontificia Universidad Católica del Ecuador Ibarra). content (puce.edu.ec)

Macías-Lara, R. A., Andrade, M. F. B., Angulo, F. Q., Loor, J. J. M., Estupiñan-Troya, G., & Vizuete, J. D. R. (2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(2), 231-243. Frequent cases, criminalization and prevention of computer crimes in Ecuador: a brief systematic review | Sapienza: International Journal of Interdisciplinary Studies (sapienzaeditorial.com)

Peña Murillo, K. M. (2023). *Suplantación de identidad en las redes sociales en la ciudad de Babahoyo en 2023* (Bachelor's thesis). DSpace de Uniandes: Suplantación de identidad en las redes sociales en la ciudad de Babahoyo en 2023

Porras Montufar, R. X. (2023). Análisis de las actividades ciberdelictivas desarrolladas en el Ecuador, durante el período 2020-2021. Análisis de las actividades ciberdelictivas desarrolladas en el Ecuador, durante el período 2020-2021 (uexternado.edu.co)

Saltos Pinto, H. G. (2022). *Abordaje de la prevención del delito cibernético y el derecho a la intimidad en Ecuador* (Bachelor's thesis, Quito, Universidad Metropolitana). Repositorio Digital UMET: Abordaje de la prevención del delito cibernético y el derecho a la intimidad en Ecuador.

En el año 2019, los habitantes ecuatorianos quedaron sin protección frente a los ciberdelincuentes, hicieron que las autoridades tomaron acciones como la promulgación de la Ley Orgánica de Protección de Datos Personales y las reformas del COIP. https://repositorio.urnet.edu.ec/handle/67000/192