UNIVERSIDAD LAICA VICENTE ROCAFUERTE
DE GUAYAQUIL
FACULTAD DE CIENCIAS SOCIALES Y DERECHO
CARRERA DE DERECHO

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

ABOGADO/A

TEMA

SUPLANTACIÓN DE IDENTIDAD CIBERNÉTICA: IMPACTO EN LA SEGURIDAD DIGITAL

TUTOR

Mgtr. EDUARDO JOSÉ MEDINA MAZZINI

AUTORES

ALISSON SOLANGE CORDOVA NOGUERA

CHARLES ANDRES MORENO RENJIFO

GUAYAQUIL, 2025

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA	
FICHA DE REGISTRO DE TESIS	
TÍTULO Y SUBTÍTULO: SUPLANTACIÓN DE IDENTIDAD CIBERNÉTICA: IMPACTO EN LA SEGURIDAD DIGITAL	
AUTOR/ES: Cordova Noguera Alisson Solange. Moreno Renjifo Charles Andres.	**TUTOR:** Mgtr. Medina Mazzini Eduardo José.
INSTITUCIÓN: Universidad Laica Vicente Rocafuerte de Guayaquil	**Grado obtenido:** Abogado
FACULTAD: CIENCIAS SOCIALES Y DERECHO.	**CARRERA:** DERECHO.
FECHA DE PUBLICACIÓN: 2025	**N. DE PÁGS:** 100.
ÁREAS TEMÁTICAS: Derecho.	
PALABRAS CLAVE: Identidad, protección de datos, seguridad, derecho, derecho a la privacidad.	

RESUMEN:

El presente trabajo investigativo tiene como objetivo principal detectar cuales son los factores que conllevan a la suplantación de identidad y los diferentes ataques cibernéticos que varios usuarios se ven afectados. En la actualidad la era digital se ha convertido en una amenaza directa para los individuos, empresas e incluso a los gobiernos. La suplantación de identidad crea el uso no autorizado de información personal para obtener beneficios ilícitos, por ende, los ataques cibernéticos comprometen con la seguridad de los sistemas informáticos e incluso robar información que afecte hasta la integridad de una persona. Dentro del análisis investigativo, varios expertos en el tema legal mencionaron lo importante de hacer uso adecuado de los diferentes sitios web al momento de expones datos personales que sean el causante para vernos expuestos ante estas estafas cibernéticas.

El enfoque que tuvo la investigación cualitativa permitió comprender los diferentes fenómenos sociales identificando las ventajas y desventajas que una

<table>
<tr><td colspan="3">persona se expone de manera directa. En la propuesta se busca implementar estrategias sólidas y efectivas como la educación y campañas de analfabetismo digital, una ley que ampare a las víctimas velando por sus intereses, y, acogernos a modelos internacionales donde se fortalezca de una manera directa al país.</td></tr>
<tr><td>N. DE REGISTRO (en base de datos):</td><td colspan="2">N. DE CLASIFICACIÓN:</td></tr>
<tr><td colspan="3">DIRECCIÓN URL (Web):</td></tr>
<tr><td>ADJUNTO PDF:</td><td>SI [X]</td><td>NO [ ]</td></tr>
<tr><td>CONTACTO CON AUTOR/ES:
Cordova Noguera Alisson Solange

Moreno Renjifo Charles Andres</td><td>Teléfono:
0993329591

0987804894</td><td>E-mail:
acordovan@ulvr.edu.ec

cmorenor@ulvr.edu.ec</td></tr>
<tr><td>CONTACTO EN LA INSTITUCIÓN:</td><td colspan="2">Mgtr. Carlos Manuel Pérez Leyva (Decano)
Teléfono: (04) 259 6500 Ext. 249
E-mail: cperezl@ulvr.edu.ec
Mgtr. Geancarlos Steven Gonzalez Solorzano (Director de Carrera)
Teléfono: (04) 259 6500 Ext. 233
E-mail: ggonzalezso@ulvr.edu.ec</td></tr>
</table>

CERTIFICADO DE SIMILITUD

CERTIFICADO DE ANÁLISIS
magister

2TESIS CORDOVA NOGUERA ALISSON, MORENO RENJIFO CHARLES (2)

5% Textos sospechosos

- 5% **Similitudes**
  - < 1% similitudes entre comillas
  - 0% entre las fuentes mencionadas
- < 1% **Idiomas no reconocidos (ignorado)**
- 5% **Textos potencialmente generados por la IA (ignorado)**

Nombre del documento: 2TESIS CORDOVA NOGUERA ALISSON, MORENO RENJIFO CHARLES (2).pdf
ID del documento: 2592efc9dcbd1af186b0b5d86df8a1c4f7d7c2a9
Tamaño del documento original: 1,02 MB

Depositante: EDUARDO JOSÉ MEDINA MAZZINI
Fecha de depósito: 20/8/2025
Tipo de carga: interface
fecha de fin de análisis: 20/8/2025

Número de palabras: 15.401
Número de caracteres: 102.456

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**www.lexis.com.ec** | Ley Orgánica de Protección de Datos Personales | Descargar... https://www.lexis.com.ec/biblioteca/ley-organica-proteccion-datos-personales **1 fuente similar**	1%		Palabras idénticas: 1% (209 palabras)
2	**www.ministeriodegobierno.gob.ec** | Las redes sociales son un 'arma' utilizada p... https://www.ministeriodegobierno.gob.ec/las-redes-sociales-son-un-arma-utilizada-por-estru...	< 1%		Palabras idénticas: < 1% (125 palabras)
3	**Documento de otro usuario** #f16ccc Viene de de otro grupo **10 fuentes similares**	< 1%		Palabras idénticas: < 1% (99 palabras)
4	**doi.org** | Estrategias innovadoras para mitigar la suplantación de identidad en re... https://doi.org/10.60100/rcmg.v5i1.212	< 1%		Palabras idénticas: < 1% (87 palabras)
5	**coggle.it** | Investigación Cualitativa., image, image, image, image, image - Coggle... https://coggle.it/diagram/aBWj58eQzBRMLyUg/t/investigación-cualitativa **3 fuentes similares**	< 1%		Palabras idénticas: < 1% (69 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repositorioslatinoamericanos.uchile.cl** | Machine Learning in the detection of e... https://repositorioslatinoamericanos.uchile.cl/handle/2250/5418351	< 1%		Palabras idénticas: < 1% (38 palabras)
2	**www.aepd.es** https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf	< 1%		Palabras idénticas: < 1% (30 palabras)
3	**localhost** | Delitos informáticos. reforma al artículo 190 del COIP en el contexto d... http://localhost:8080/xmlui/bitstream/redug/50908/3/Jonathan Morán - Ruth Morán BDER-TP...	< 1%		Palabras idénticas: < 1% (22 palabras)
4	**www.telecomunicaciones.gob.ec** https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Resumen.pdf	< 1%		Palabras idénticas: < 1% (11 palabras)
5	**maria-pascual.es** | Estrategias Efectivas para la Prevención de Vulnerabilidades e... https://maria-pascual.es/prevencion-de-vulnerabilidades-en-aplicaciones-moviles/#:~:text=¿C...	< 1%		Palabras idénticas: < 1% (10 palabras)

Eduardo Jose Medina Mazzini
Time Stamping Security Data

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES

Los estudiantes egresados ALISSON SOLANGE CORDOVA NOGUERA Y CHARLES ANDRES MORENO RENJIFO, declaramos bajo juramento, que la autoría del presente Trabajo de Titulación, “Suplantación de Identidad Cibernética: Impacto en la Seguridad Digital”, corresponde totalmente a los suscritos y nos responsabilizamos con los criterios y opiniones científicas que en el mismo se declaran, como producto de la investigación realizada.

De la misma forma, cedemos los derechos patrimoniales y de titularidad a la Universidad Laica VICENTE ROCAFUERTE de Guayaquil, según lo establece la normativa vigente.

Autores,

Firma: 

ALISSON SOLANGE CORDOVA NOGUERA

C.I.1721807822

Firma: 

CHARLES ANDRES MORENO RENJIFO

C.I. 0956732275

CERTIFICACIÓN DE ACEPTACIÓN DEL DOCENTE TUTOR

En mi calidad de docente Tutor del Trabajo de Titulación **"Suplantación de Identidad Cibernética: Impacto en la Seguridad Digital"**, designado por el Consejo Directivo de la Facultad de Ciencias Sociales y Derecho de la Universidad Laica VICENTE ROCAFUERTE de Guayaquil.

CERTIFICO:

Haber dirigido, revisado y aprobado en todas sus partes el Trabajo de Titulación, titulado**: "Suplantación de Identidad Cibernética: Impacto en la Seguridad Digital"**, presentado por los estudiantes **ALISSON SOLANGE CORDOVA NOGUERA Y CHARLES ANDRES MORENO RENJIFO** como requisito previo, para optar al **Título de Abogado**, encontrándose apto para su sustentación.

Firma: 

EDUARDO JOSÉ MEDINA MAZZINI

C.C. 0918078924

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a Dios por guiarme, cuidarme y protegerme a lo largo de mis estudios así mismo poder culminarlos exitosamente de la mano de él, otorgándome la sabiduría para siempre destacar lo mejor de mí. Y permitir que junto a mi familia podamos compartir la culminación de esta importante etapa.

A mi querida madre la Lic. Soraya Noguera por su apoyo incondicional y esfuerzo. Gracias por estar siempre a mi lado celebrando mis logros.

A mis hermanos Jendrik y Junior, su presencia ha sido un abrazo constante en este recorrido.

Al Sr. Carlos Vega, su apoyo incondicional ha sido fundamental para mí.

A mi compañero de tesis, por su apoyo y compromiso, que hicieron posible desarrollar este proyecto de la mejor manera.

Alisson Solange Cordova Noguera

Con infinita gratitud a Dios por ser mi guía en cada paso de este camino.

Gracias a mis papás quiénes han sabido formarme con buenos valores, y cada paso de este camino lo he dado con el apoyo de sus palabras y su confianza en mí.

A mis tías Andrea Moreno Silva; Nataly Moreno Silva y a mi tío Adrián Moreno Silva por estar presente y darme su apoyo incondicional.

su perseverancia y su esfuerzo de salir adelante, han sido mi respaldo en cada etapa de este proceso, los admiro y estoy muy orgulloso de ustedes.

Gracias a mi compañera quien se ha convertido en un pilar fundamental en mi vida, el cual marco un antes y un después. Se que la vida nos depara grandes momentos juntos.

Charles Andres Moreno Renjifo

DEDICATORIA

Le Dedico a Dios quien ha sido mi guía y me ha protegido, ser foránea no ha sido fácil, pero con su fortaleza me ha sostenido a no desistir en el camino.

A mí, por el empeño y dedicación a lo largo de la carrera universitaria.

A mis seres queridos: mi madre por su amor incondicional y apoyo inquebrantable; mis hermanos Jendrik y Junior; al Sr. Carlos Vega;

A mi angelito en el cielo, mi padre Edwin Cordova, aunque no estas físicamente, siempre te llevo en mi pensamiento y en mi corazón.

Este logro es fruto de su amor, apoyo y esfuerzo. Con todo mi corazón, les dedico este logro.

Alisson Solange Cordova Noguera

En primer lugar, a mí mismo, por recordarme que cada sacrificio valió la pena. Hoy, celebro no solo el final de un capítulo, sino el comienzo de un futuro brillante que yo mismo he construido.

A mi abuela Andrea Silva Zambrano, la persona que creyó en mí desde el principio. Gracias por cada palabra de aliento y por guiar mis pasos en mis estudios. Esto es por ti.

Se lo dedico a mis padres Charles Omar Moreno Silva y Sandra Elizabeth Renjifo Marquez; que en el transcurso de mi vida me supieron inculcar valores y confiaron en mi persona y en mis deseos de superación Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi capacidad. Es por ello que soy lo que soy ahora. Los amo con mi vida.

Charles Andres Moreno Renjifo

RESUMEN

El presente trabajo investigativo tiene como objetivo principal detectar cuales son los factores que conllevan a la suplantación de identidad y los diferentes ataques cibernéticos que varios usuarios se ven afectados. En la actualidad la era digital se ha convertido en una amenaza directa para los individuos, empresas e incluso a los gobiernos. La suplantación de identidad crea el uso no autorizado de información personal para obtener beneficios ilícitos, por ende, los ataques cibernéticos comprometen con la seguridad de los sistemas informáticos e incluso robar información que afecte hasta la integridad de una persona. Dentro del análisis investigativo, varios expertos en el tema legal mencionaron lo importante de hacer uso adecuado de los diferentes sitios web al momento de expones datos personales que sean el causante para vernos expuestos ante estas estafas cibernéticas.

El enfoque que tuvo la investigación cualitativa permitió comprender los diferentes fenómenos sociales identificando las ventajas y desventajas que una persona se expone de manera directa. En la propuesta se busca implementar estrategias sólidas y efectivas como la educación y campañas de analfabetismo digital, una ley que ampare a las víctimas velando por sus intereses, y, acogernos a modelos internacionales donde se fortalezca de una manera directa al país.

PALABRAS CLAVES:

Identidad, data protection, seguridad, derecho, derecho a la privacidad.

ABSTRACT

The main objective of this research is to identify the factors that lead to identity theft and the various cyberattacks that affect various users. Today, the digital age has become a direct threat to individuals, businesses, and even governments. Identity theft creates the unauthorized use of personal information for illicit gain. Therefore, cyberattacks compromise the security of computer systems and even steal information that even affects a person's integrity. Within the investigative analysis, several legal experts mention the importance of making appropriate use of different websites when exposing personal data that could lead to exposure to these cyber scams.

The qualitative research approach allowed us to understand different social phenomena by identifying the advantages and disadvantages to which a person is directly exposed. The proposal seeks to implement solid and effective strategies such as education and digital literacy campaigns, a law that protects victims and safeguards their interests, and adopts international models that directly strengthen the country.

KEY WORDS:

Identity, digital, security, law, right to privacy.

ÍNDICE GENERAL

Índice de tablas

Índice de Anexos

INTRODUCCIÓN

La suplantación de identidad cibernética representa uno de los desafíos más complejos y apremiantes en el ámbito de la seguridad digital, constituyendo una amenaza en muchas facetas que trasciende las fronteras, afectan tanto la integridad personal como la estabilidad de los sistemas digitales globales. Esta problemática que ha experimentado un crecimiento exponencial con la digitalización numerosa de los servicios y la red global característica del siglo XXI.

En Ecuador al igual que el resto del mundo este fenómeno representa una amenaza constante tanto en los servicios públicos o privados. Esta investigación tiene como objetivo analizar el impacto que este fenómeno tiene y analizar las normativas legales y mecanismos de protección de datos de los ciudadanos, en estas se encuentra la Constitución de la Republica del Ecuador, la Ley Orgánica de Protección de Datos Personales, el Código Integral Penal asimismo se incluye el derecho comparado con normativa internacional.

La elección de este tema busca analizar de manera integral el impacto que genera el entorno de seguridad digital, desde las afectaciones individuales hasta las persecuciones sistemáticas que pueden comprometer la confianza en las plataformas digitales y los servicios en línea.

CAPÍTULO I

ENFOQUE DE LA PROPUESTA

1.1.Tema:

Suplantación de Identidad Cibernética y su Impacto en la Seguridad Digital

1.2.Planteamiento del Problema:

El presente estudio investiga la “Suplantación de identidad cibernética: Impacto en la seguridad digital”. Para la realización del problema se procedió a realizar un estudio previo en los diferentes repositorios de tesis, artículos, revistas como Dialnet y Flacso de las distintas universidades que tiene el país.

Durante los últimos años, se ha estado viviendo una época de la era digital las nuevas formas de comunicarse, de realizar trámites, de conocer personas por medio de las redes o plataformas digitales ha causado un gran impacto y un peligro por las diferentes formas de estafar y suplantar la identidad de una persona. Ecuador se ha enfrentado a una creciente amenaza en el ámbito de ciberseguridad, donde la suplantación cibernética se ha consolidado como uno de los delitos digitales más prevalentes y perjudiciales. El país se encuentra en una posición vulnerable ante los ataques cibernéticos en el contexto sudamericano, mientras que las estafas y suplantación de identidad constituyen los principios cibernéticos según la Policía Nacional.

La dimensión del problema se evidencia en múltiples aspectos críticos. Ecuador se posiciona entre los países con mayor incidencia de ataques cibernéticos en América Latina, junto con Brasil y México. La vulnerabilidad de la población se ve agrada por el hecho de que el 8.2% de ecuatorianos son analfabetos digitales, los que los hace especialmente vulnerables a estos delitos (Machado, 2024).

1.3.Formulación del Problema:

¿Cuál es el impacto de la suplantación de identidad cibernética en la seguridad digital del Ecuador y que modalidades implementan los delincuentes?

1.4. Objetivo General

Analizar el impacto social de la suplantación de identidad, la normativa legal y la protección de datos de los ciudadanos en el Ecuador.

1.5.Objetivos Específicos

•Identificar las principales modalidades más frecuentes de la suplantación de identidad cibernética.

•Analizar el marco legal ecuatoriano vigente sobre de prevención y sanción de este delito.

•Examinar los factores que facilitan la suplantación de identidad, incluyendo la falta de educación digital y falta de seguridad en las plataformas.

1.6.Idea a Defender

La suplantación de identidad representa una amenaza evolutiva para la seguridad digital de los ciudadanos en el Ecuador, debido a la combinación de factores como la falta de educación digital, deficiencias en la seguridad de las plataformas digitales.

1.7.Línea de Investigación Facultad:

Línea de investigación de facultad: Sociedad civil, derechos humanos y gestión de la comunicación adicional la línea de investigación de la carrea: Derecho digital y las tecnologías de la información y la comunicación.

CAPÍTULO II

MARCO REFERENCIAL

2.1. Marco Teórico

La suplantación de identidad cibernética llega como una modalidad de delito digital con el objetivo de obtener información confidencial, acceder a recursos restringidos o cometer los diferentes fraudes. Las herramientas digitales permiten la creación de perfiles falsos en redes sociales, sitios web y servicios en línea con relativa facilidad. Se ha investigado sobre factores que caracterizan a los usuarios que intentan suplantar la identidad en redes sociales, identificando indicadores claves como la cantidad de publicaciones, el uso de fotos de perfil inusuales y la presencia de perfiles repetidos. (Macías Lara R. A., 2024)

Es fundamental analizar cuáles son los factores que contribuyen a la suplantación de identidad. La revolución de la nueva era digital tuvo un impacto considerable en las formas de interactuar por medio de una pantalla con varias personas, sin medir los diferentes riesgos que llegue a ocasionar como publicar la dirección del domicilio, colocar información relevante en los diferentes perfiles digitales.

El uso malicioso de las redes sociales en la sociedad de la información ha generado la aparición de un nuevo escenario criminal que se ha denominado el mundo virtual, en donde no se aplican los conceptos de tiempo y espacio, al igual que en el mundo real y esto ha ocasionado un sinfín de interrogantes y vacíos jurídicos. Uno de esos usos maliciosos de las redes sociales constituye la creación de perfiles falsos, que jurídicamente crea una forma de suplantación de la identidad personal en redes sociales. Son víctimas de este hecho tanto personas físicas como jurídicas y los fines ilícitos son generalmente el perjuicio moral o patrimonial (Acevedo, 2027, p.18).

> Según la revista DataReportal (2025) menciona que “a inicios del presente año Ecuador tuvo 15.2 millones de personas utilizando internet, la penetración en línea es del 83.7% las oportunidades para la suplantación de identidad en plataformas digitales se multiplican exponencialmente” (p.8).

Es importante recalcar que cada individuo debe darle un buen uso a su red social o plataforma digital, es por ello, que proteger la información personal es responsabilidad de cada sujeto. Es preciso usar las redes sociales de una manera responsable cuidando la información personal el cual, se evita ser víctima de una suplantación de identidad y proteger la seguridad digital.

2.1.1 Factores que facilitan la suplantación de identidad

La suplantación de identidad cibernética representa uno de los delitos digitales más prevalentes en la actualidad, afectando a millones de personas en todo el mundo. Este fenómeno criminal se caracteriza por el uso no autorizado de información personal de terceros para cometer fraudes, acceder a servicios, o causar daño reputacional. Su crecimiento exponencial en los últimos años no es casualidad, sino el resultado de la confluencia de múltiples factores que han creado un ecosistema digital especialmente vulnerable a este tipo de ataques.

Entre los factores facilitadores más relevantes se encuentra la masiva digitalización de datos personales, que ha resultado en la creación de vastos repositorios de información sensible almacenada en sistemas con diferentes niveles de seguridad. La proliferación de plataformas digitales y redes sociales ha multiplicado los puntos de acceso a información personal, mientras que las brechas de seguridad en organizaciones públicas y privadas han expuesto millones de registros de datos personales.

Se trata de un delito facilitado por diversos factores, muchos de los cuales están relacionados con la falta de precauciones, tanto a nivel personal como en la seguridad de los sistemas digitales. Los principales factores que contribuyen a este problema son:

2.1.1.1. Analfabetismo digital

Las personas con limitaciones en competencias digitales son especialmente susceptibles a técnicas de ingeniería social como el phishing, donde correos electrónicos o mensajes fraudulentos imitan comunicaciones legítimas de bancos u otras instituciones.

Las comunidades con menor acceso a educación tecnológica y recursos digitales presentan mayor vulnerabilidad a ataques de suplantación de identidad. Esta

brecha se amplifica en contextos donde la transformación digital ha sido acelerada sin acompañamiento educativo adecuado.

Los adultos mayores representan un segmento particularmente vulnerable debido a su menor familiaridad con tecnologías digitales y mayor confianza en comunicaciones que parecen oficiales. Sin embargo, el analfabetismo digital también afecta a usuarios jóvenes que, pese a su aparente facilidad tecnológica, carecen de conocimientos sobre privacidad y seguridad digital.

Para (Álvarez et al., 2020) “el analfabetismo se convierte en la incapacidad de que un cierto determinado grupo de personas usen de una manera adecuada las diferentes herramientas tecnológicas”.

La falta de educación en ciberseguridad y alfabetización digital en las escuelas y en los hogares contribuye a esta problemática, ya que los jóvenes no cuentan con los conocimientos necesarios para proteger su información en línea. Es vital impulsar mecanismos de alfabetización y de apropiación digital que permitan un amplio aprovechamiento de las oportunidades que ofrece la red, pero desde una perspectiva con criterio propio, en la que el usuario esté en capacidad de comprender el impacto de su huella digital.

Una de las principales intenciones de esta investigación era el brindar potenciales estrategias de alfabetización digital que permitieran a las juventudes colombianas contar con herramientas para afrontar peligros en el entorno digital, por ello, para abordar opciones a parte de las ya disponibles como seminarios (Díaz, 2024).

2.1.1.2 Uso indebido de redes sociales

Las redes sociales han transformado radicalmente la forma en que compartimos información personal, creando un ecosistema digital donde la sobreexposición de datos privados facilita considerablemente el robo de identidad. El uso indebido de estas plataformas por parte de los usuarios crea vulnerabilidades que los ciberdelincuentes explotan sistemáticamente.

Muchos usuarios mantienen perfiles completamente públicos o con configuraciones de privacidad permisivas, permitiendo que desconocidos accedan a información personal extensa. La falta de comprensión sobre las opciones de

privacidad disponibles, combinada con la complejidad cambiante de estas configuraciones, resulta en exposición involuntaria de datos sensibles.

Las contraseñas débiles o reutilizadas en varias cuentas son una puerta de entrada clave para los estafadores. La falta de autenticación de dos factores, la conexión a redes wifi públicas no seguras y la falta de actualización de software y dispositivos con los parches de seguridad más recientes crean vulnerabilidades que los delincuentes aprovechan fácilmente.

Según los autores (Echeburúa & Corral, 2010) hacen referencia al abuso de las tecnologías de la información y la comunicación. Citan lo siguiente:

“Los riesgos más importantes del abuso de las TIC son, además de la adicción, el acceso a contenidos inapropiados, el acoso o la pérdida de intimidad. Así, en las redes se puede acceder a contenidos pornográficos o violentos o transmitir mensajes racistas, proclives a la anorexia, incitadores al suicidio o a la comisión de delitos” (p, 92).

La sobreexposición de información personal es quizás el error más frecuente. Los usuarios comparten detalles íntimos de su vida, ubicaciones en tiempo real, datos familiares y profesionales sin considerar que esta información puede ser recopilada y utilizada maliciosamente. Los ciberdelincuentes aprovechan estas publicaciones para construir perfiles detallados de sus víctimas.

La creación de perfiles falsos se ha sofisticado considerablemente. Los estafadores utilizan fotografías robadas, información personal obtenida de diversas fuentes y técnicas de ingeniería social para crear identidades convincentes que les permiten ganarse la confianza de otros usuarios.

Es fundamental configurar cuidadosamente las opciones de privacidad, limitando quién puede ver la información personal y las publicaciones. Los usuarios deben revisar regularmente estas configuraciones, ya que las plataformas a menudo actualizan sus políticas de privacidad.

La verificación de contactos es crucial antes de aceptar solicitudes de amistad o compartir información sensible. Es recomendable confirmar la identidad de las personas a través de múltiples canales antes de establecer contacto.

2.1.1.3 Vulneración en redes sociales

La vulneración de seguridad en redes sociales constituye uno de los vectores más críticos para la obtención masiva de información personal utilizada en esquemas de suplantación de identidad. Estas brechas exponen datos sensibles de millones de usuarios, proporcionando a los criminales cibernéticos recursos extensos para perpetrar fraudes sofisticados.

Por otra parte, también resulta importante señalar que, si se viola la privacidad de un usuario, el sistema toma las medidas adecuadas para evitarlo o, si es inevitable, al menos informa al usuario para que pueda abordar la violación, en las redes sociales en línea actuales, se espera que los usuarios controlen cómo circula su contenido en el sistema y averigüen manualmente si se ha violado su privacidad. Esto, desde luego, resulta la mayoría de las veces poco práctico e incluso puede resultar hasta cierto punto imposible de detectar o de manejar adecuada y oportunamente (Herrera, 2017, p.124).

Los atacantes aprovechan las configuraciones de privacidad deficientes que muchos usuarios mantienen por desconocimiento. Perfiles completamente públicos proporcionan información valiosa para ataques de ingeniería social, permitiendo a los delincuentes construir estrategias personalizadas de manipulación.

2.1.2. Riesgos

Los riesgos son las consecuencias negativas y los peligros que enfrenta una persona cuando su información personal es robada y utilizada fraudulentamente. Estos riesgos afectan no solo el ámbito financiero, sino también el personal y el profesional.

(Macías Lara R. A., 2024) se refiere que:

Al mitigar los riesgos de suplantación de identidad y otros delitos cibernéticos, se fortalece la confianza en las plataformas en línea y se fomenta un entorno digital más inclusivo y accesible para todos. En última instancia, la colaboración entre individuos, empresas, gobiernos y profesionales de seguridad cibernética es

fundamental para mantener la integridad y la confianza en un mundo digital en constante cambio. Este enfoque proactivo no solo protege la integridad de los usuarios, sino que también fortalece la confianza en las plataformas en línea, fomentando así un entorno digital más seguro y fiable para todos (pp. 544 – 561).

Las víctimas enfrentan pérdidas económicas directas que pueden incluir vaciado de cuentas bancarias, uso fraudulento de tarjetas de crédito, contratación no autorizada de préstamos, y apertura de cuentas financieras maliciosas.

2.1.2.1 Phishing

Phishing es la combinación de Ingeniería Social y exploit técnicos, diseñados para convencer a una víctima de proporcionar información personal, generalmente realizado para obtener una ganancia monetaria por parte del atacante. La mayoría de los ataques de Phishing son influenciados cuando se envía un correo electrónico falso, que contiene un enlace (Uniform Resource Locator, URL). Esta URL conduce a un sitio web falso, cuando se hace clic en él. A pesar de la importante atención que se le ha otorgado a lo largo de los años, aún no existe una solución definitiva, para resolver este tipo de ataque (Benavides, 2020).

La suplantación de identidad cibernética en Ecuador adopta múltiples formas. Entre ellas se encuentran la creación de cuentas falsas en plataformas sociales, el envío de correos electrónicos engañosos (phishing) para obtener información, el acceso no autorizado a datos bancarios y el empleo de información personal robada para llevar a cabo estafas financieras.

2.1.2.2 Smishing

Es un tipo de cibercrimen que surge con la función entre “SMS” y “phishing”, caracterizado por el uso de mensajes de texto maliciosos enviados a teléfonos móviles. Su propósito principal es manipular a los usuarios para que compartan datos confidenciales como claves de acceso, información bancaria, detalles de tarjetas de crédito o datos de identidad personal.

Los textos fraudulentos suelen incluir vínculos peligrosos que redirigen hacia páginas web falsificadas, creadas para simular sitios auténticos de entidades financieras, sistemas de pago, plataformas sociales o tiendas en línea. Estas réplicas

maliciosas están elaboradas específicamente para robar las credenciales que los usuarios proporcionan al pensar que están interactuando con un servicio verdadero.

Las consecuencias del smishing pueden ser devastadoras para las víctimas. El robo de identidad es una de las consecuencias más graves, pudiendo llevar años resolver completamente. Los atacantes pueden utilizar la información robada para abrir cuentas bancarias, solicitar préstamos, realizar compras fraudulentas o cometer otros delitos en nombre de la víctima.

El impacto financiero directo también es significativo. Las víctimas pueden perder dinero de sus cuentas bancarias, enfrentar cargos no autorizados en sus tarjetas de crédito, o encontrarse con deudas que no contrajeron. Además del impacto financiero inmediato, las víctimas a menudo deben invertir tiempo y recursos considerables para restaurar su identidad y credibilidad financiera.

El impacto psicológico no debe subestimarse. Las víctimas de smishing frecuentemente experimentan estrés, ansiedad, y una pérdida de confianza en la tecnología y las comunicaciones digitales. Esta desconfianza puede afectar su capacidad para utilizar servicios digitales legítimos en el futuro.

2.1.2.3 Vishing

Es una forma sofisticada de ciberataque que combina las palabras (voz) y "phishing", consistiendo en el uso de llamadas telefónicas fraudulentas para engañar a las víctimas y obtener información personal sensible, como datos bancarios, números de seguridad social, contraseñas, o información de tarjetas de crédito. A diferencia del phishing tradicional que utiliza correos electrónicos, o del smishing que emplea mensajes de texto, el vishing aprovecha la comunicación vocal directa para crear una sensación de legitimidad y urgencia que puede ser particularmente efectiva para manipular a las víctimas.

La suplantación de identificador de llamadas (caller ID spoofing) es una técnica fundamental que permite a los atacantes hacer que sus llamadas parezcan provenir de números telefónicos legítimos de organizaciones conocidas. Esta técnica puede hacer que una llamada fraudulenta aparezca como proveniente del banco local de la víctima o de una agencia gubernamental reconocida.

Los atacantes de vishing utilizan diversos métodos para identificar y seleccionar a sus víctimas. Algunos emplean enfoques de "disparo masivo",

realizando miles de llamadas aleatorias con la esperanza de encontrar víctimas susceptibles. Otros utilizan bases de datos obtenidas ilegalmente que contienen información personal detallada, permitiéndoles personalizar sus ataques y aumentar significativamente las tasas de éxito.

Pero quienes difunden estos datos, En Ecuador, la información privada de las personas es difundida principalmente por entidades del sector público y privado que manejan datos personales. La difusión ilegal de esta información puede provenir de organizaciones o incluso de individuos dentro de estas instituciones que no cumplen con las normativas de protección de datos.

2.1.2.4 Cookies

Las cookies son pequeños archivos de texto que los sitios web almacenan en el dispositivo del usuario (computadora, smartphone, Tablet) cuando se navega por internet. Estos archivos contienen información específica sobre la interacción del usuario con el sitio web y se envían de vuelta al servidor cada vez que el usuario visita nuevamente esa página.

Son el recolector de informacion sobre los diferentes habitos de navegación que se tiene el acceso de crear perfiles e indicar cierta informacion tipificada, que conlleva a una invasión de privacidad.

Las ‘cookies’ pueden ser explotadas por ciberdelincuentes para espiar tu actividad en línea y acceder a información personal. Estos pequeños fragmentos son enviados al navegador cuando se realiza una visita en cualquier tipo de contenido que se acceda.

Unas de las maneras para evitar las cookies son las siguientes:

- Configura tu navegador: Puedes configurar tu navegador para que las bloquee o te avise cada vez que un sitio web intente almacenar una en tu dispositivo (Jimenez, 2024).
- Navegacion en modo incognito.
- Eliminar cookies periodicamente
- Desactivar o eliminar el almacenamiento local y caché

Por lo tanto, gestionar adecuadamente las cookies permite a los usuarios proteger sus datos personales, mantener su identidad digital segura y reducir el riesgo de seguimiento no deseado o suplantación de identidad.

2.1.3. Impacto

El impacto de internet y las herramientas digitales en la suplantación de identidad cibernética es profundo y multifacético, facilitando tanto la comisión de estos delitos como el desarrollo de nuevas estrategias para combatirlos.

En la sociedad se ve altamente transformado la facilidad de poder comunicarse entre varios usuarios, se han habilitado estrategias de trabajos virtuales, al mismo tiempo también ha tenido un aumento de sofisticación y los costos de ataques cibernéticos. Tal como lo menciona (Maldonado & Medina, 2023) por los diferentes ataques se están tomando medida para prevenir y combatir los ciberdelitos las diferentes iniciativas tanto públicas como privadas buscan tener una seguridad digital.

Los sistemas de autenticación y verificación enfrentan desafíos sin precedentes ante la suplantación cibernética. Los mecanismos tradicionales de verificación basados en conocimiento (contraseñas, preguntas de seguridad) o posesión (dispositivos móviles, tarjetas) pueden ser comprometidos mediante ingeniería social sofisticada o ataques técnicos dirigidos.

2.1.4. Afectaciones a la privacidad

Reconocer las afectaciones a la privacidad refuerza la necesidad de educar a los usuarios en prácticas de seguridad digital, fomentando un uso responsable de la tecnología y promoviendo una cultura de protección de datos personales.

El Internet, especialmente las redes sociales y los servicios en línea, ha facilitado la recopilación de grandes cantidades de información personal (nombres, fechas de nacimiento, direcciones, hábitos, contactos, etc.) que los ciberdelincuentes pueden utilizar para construir perfiles falsos o para llevar a cabo ataques de ingeniería social más convincentes. Algunos estudios, como el de (Burt, 2020, como se citó citado en la revista científica multidisciplinar Generando) señala la importancia de analizar datos de ataques cibernéticos y comportamientos delictivos en línea para comprender las tendencias y patrones de la suplantación de identidad.

2.1.5 Delitos

Son actos ilegales que ocurren cuando una persona usa la información personal de otra sin su consentimiento para cometer un fraude, causar daño u obtener un beneficio. Estos crímenes no se limitan a robar una identidad, sino que se manifiestan a través de una variedad de acciones delictivas que usan la tecnología como herramienta.

2.1.5.1 Estafa

La estafa constituye uno de los delitos más frecuentes y lucrativos dentro de los esquemas de suplantación de identidad cibernética, representando la materialización económica del uso fraudulento de identidades ajenas para obtener beneficios patrimoniales ilícitos, los suplantadores crean tiendas virtuales falsas, publican productos inexistentes en plataformas de venta, o establecen transacciones comerciales utilizando identidades legítimas robadas.

Las estafas digitales están en auge en Ecuador, con un preocupante incremento de denuncias. En 2024, la fiscalía general del Estado registró 3.913 casos de delitos informáticos en el sistema financiero, un promedio de 326 mensuales y un aumento del 7 % respecto a 2023. El primer trimestre de 2025 ya suma 831 denuncias.

Pichincha, Guayas y Manabí son las provincias más afectadas. “El 94 % de los casos en 2024 fueron por apropiación fraudulenta por medios electrónicos, delito sancionado por el artículo 190 del COIP con uno a tres años de prisión” (El Oriente, 2025, p. 3).

Un caso reciente conmociona por su gravedad. Juana María Pérez (nombre protegido por seguridad) recibió una citación de la Fiscalía en enero de 2025 por presuntas llamadas de extorsión realizadas desde líneas telefónicas registradas a su nombre. El hecho la vinculaba injustamente con un temido grupo de delincuencia organizada (GDO) que operaba en Guayaquil. Las investigaciones revelaron que, en septiembre de 2024, delincuentes compraron nueve líneas prepago utilizando su número de cédula sin su consentimiento. Hasta ahora, no se ha determinado cómo accedieron a su información personal. (Zambrano, 2025)

2.1.5.2 Estafa en la red social WhatsApp

Este caso involucra a un estafador que busca tomar el control de tu cuenta de WhatsApp haciéndose pasar por un amigo o familiar para que entregues un código de verificación. El delincuente utiliza su propio dispositivo o una cuenta robada para enviar mensajes aparentando ser alguien cercano a ti. Al mismo tiempo, activan el proceso de verificación de WhatsApp que genera seis dígitos enviados por SMS o correo electrónico. Luego figuen que ese código fue enviado por error y te piden que se lo reenvíes. Si accedes y compartes el código, el estafador obtiene el acceso total a tu cuenta, perdiéndole acceder a tus contactos y leer tus mensajes privados. (De Aplicación Docente, D.D, 2024)

Los ataques dirigidos a familiares representan una de las formas más crueles de explotación. Los estafadores, una vez que han suplantado una identidad, contactan a familiares cercanos solicitando transferencias de dinero urgentes, aprovechando situaciones emocionales como emergencias médicas, problemas legales, o crisis financieras fabricadas.

Los jóvenes y adolescentes enfrentan riesgos específicos relacionados con la suplantación en contextos románticos y sociales. Los estafadores crean identidades falsas atractivas para establecer relaciones emocionales que posteriormente explotan para obtener información personal, fotografías comprometedoras, o dinero.

2.1.5.3 Fraudes financieros

Uno de los mayores peligros que enfrentan las instituciones financieras son los ataques relacionados con fraudes cibernéticos. Anualmente, estas organizaciones asumen pérdidas millonarias como consecuencia de operaciones fraudulentas. Este articulo plantea un modelo que considera los principales retos en el diseño de un sistema de detección de fraudes:

a) El marcado desequilibrio entre las clases de datos

b) La naturaleza no estacionaria de la distribución de información

c) La integración en línea del conocimiento proporcionado por los especialistas en fraudes respecto a las operaciones marcadas como dudosas.

La aplicación práctica del modelo en un conjunto de datos de prueba permitió predecir exitosamente la mayoría de los casos de transacciones fraudulentas con un mínimo porcentaje de falsos negativos (Alvarez, 2020, pp. 81-95)

A través de WhatsApp frecuentemente involucran métodos que son difíciles de rastrear o revertir, como transferencias bancarias directas o servicios de remesas. Los estafadores aprovechan la naturaleza aparentemente urgente de las solicitudes para presionar a las víctimas a utilizar métodos de pago irreversibles.

2.1.5.4 Skimming

El Skimming constituye una modalidad de fraude financiero dirigida específicamente contra tarjetas bancarias de débito y crédito. Esta técnica criminal opera mediante la extracción no autorizada de información almacenada en la banda magnética de las tarjetas, utilizando para ello equipamiento tecnológico especializado diseñado específicamente para este propósito ilícito.

La implementación del Skimming puede realizarse a través de múltiples métodos y ubicaciones, siendo los más prevalentes aquellos que se ejecutan en cajeros automáticos y terminales de punto de venta en establecimientos comerciales. El mecanismo central de esta estafa involucra la colocación estratégica de un pequeño aparato electrónico denominado skimmer, el cual posee la capacidad de interceptar, registrar y transmitir automáticamente todos los datos contenidos en las tarjetas que son procesadas a través del dispositivo comprometido.

Este sistema fraudulento permite a los delincuentes obtener información financiera sensible sin el conocimiento de las víctimas, facilitando posteriormente la realización de transacciones no autorizadas y otros tipos de fraudes económicos derivados de la información capturada ilícitamente.

Para protegernos del skimmer debemos seguir los siguientes pasos:

- Cubre el teclado con la mano cuando ingreses tu clave en cajeros automáticos.
- Mantén tu tarjeta a la vista cuando hagas un pago en cualquier establecimiento, para asegurar que solo la usaron en el dispositivo correcto.
- Fíjate si hay signos de alteración en las ranuras y teclados de los cajeros automáticos.

- Usa los cajeros ubicados en agencias y centros comerciales y evita aquellos que están aislados, ya que pueden ser más fáciles de manipular.
- Revisa con regularidad tu cuenta bancaria y extractos de la tarjeta de crédito, para detectar cualquier actividad inusual. Con Banca Móvil lo puedes hacer rápido, fácil y con total seguridad.
- Establece un monto máximo para sacar dinero por día y por operación bancaria. (Redacción Banco Pichincha , 2022)

2.1.5.5 La Pornografía Infantil

Los depredadores explotan específicamente la confianza natural de los menores en identidades digitales, aprovechando que los niños y adolescentes han crecido en entornos digitales donde las interacciones online son percibidas como normales y seguras.

La pornografía infantil no es un problema nuevo motivado por el avance tecnológico, sino que ha estado presente a lo largo de la historia. No obstante, el avance de la tecnología ha permitido la creación de nuevas formas de comunicación, lo que no sólo ha tenido efectos positivos sino también negativos ya que ha supuesto la aparición de nuevas formas de llevar a cabo este delito. “La relación de la pornografía infantil con Internet ha hecho que este delito forme parte del grupo de ciberdelitos que amenazan a la sociedad, por lo tanto, para definir la misma habrá que ubicarla en la concepción de los delitos relacionados con las nuevas tecnologías” (Salguero, 2017, p.4).

2.1.5.6 Trata de personas

La trata de personas no es una cuestión solamente de género, estatus económico o etnia. Este problema se presenta en todo el mundo y en nuestro país también. Por ello, se debe tomar medidas preventivas como: depurar la lista de contactos de redes sociales, aceptar solo a personas conocidas, no responder mensajes de desconocidos, si existen ofertas de trabajo averiguar la fuente, no confiar en publicidades informales y denunciarlas. Las organizaciones delictivas utilizan las redes sociales para captar a posibles víctimas, debido al mal uso que los usuarios dan a las mismas. El engaño es la base de este delito, mediante el cual se ofrece “oportunidades únicas” como: trabajo en el exterior con sueldos exorbitantes, dinero

fácil y sin garante, becas estudiantiles inmediatas y sin mucho papeleo (Ministerio del Gobierno, 2025).

Los tratantes han perfeccionado el uso de identidades falsas para reclutar víctimas a través de plataformas digitales. Crean perfiles convincentes en redes sociales, sitios de empleo, y aplicaciones de citas, presentándose como empleadores legítimos, agentes de modelaje, o pretendientes románticos genuinos. Estas identidades fabricadas están respaldadas por historiales digitales elaborados, fotografías robadas de personas reales, y testimonios falsos que generan credibilidad artificial.

2.1.6 Clasificación de los ciberdelitos

Para la Convención de Delitos Cibernéticos del Consejo de Europa de 2001, dentro de las acciones que son de carácter lesivo dentro de los delitos cibernéticos e informáticos los clasifica en cuatro:

1.Delitos que afecten a la privacidad y confidencialidad de un usuario vulnerando y dando un uso lesivo a los datos de las personas afectadas.

2.Delitos de fraude o falsificación.

3.Delitos en cuanto a su forma o contenido, esto corresponde directamente a la distribución de contenido ya sean fotos o videos de los usuarios sin su consentimiento o adquiridos de manera dolosa.

4.Delitos de propiedad intelectual vulnerando así el derecho de autor Bermejo & Martínez, 2020).

2.1.7 Tipos de Delitos Cibernéticos

Internet, las redes sociales y en general las tecnologías de la información y la comunicación han creado un espacio totalmente nuevo para que los niños, niñas y adolescentes aprendan y jueguen, su área de oportunidades va también de la mano con los riesgos de ser víctimas del ciberdelito, dados que estos medios permiten a los delincuentes tenerlos como su objetivo de forma individual y conjunta. Los motivos potenciales de los delincuentes incluyen la gratificación personal, generalmente mediante la explotación sexual, la creación de dinero, etc.

Las tipologías de delitos cibernéticos contra niños, niñas y adolescentes son muy variadas y también el grado de vulnerabilidad que representan para esta población, entre los más frecuentes está la pornografía infantil, el acoso cibernético

con todos sus alcances, la piratería, el tráfico de niños en línea, la extorsión en línea, el acoso sexual en línea y las diferentes variantes de violaciones de la privacidad, entre otros (Albarran, 2021, pp. 93-104).

2.1.7.1 Ciberbullying

El ciberbullying representa una forma específica de acoso digital que puede tanto facilitar como ser consecuencia de esquemas de suplantación de identidad, creando dinámicas complejas de victimización en entornos digitales.

En esta situación, uno de los riesgos al que se enfrentó el estudiante, es el ciberbullying. El acoso escolar que sucedía en las aulas se trasladó al escenario virtual, principalmente a través de las redes sociales, tal es así que en varios países ya se reportaba que los estudiantes menores de edad habían sido víctimas de este tipo de acoso (Castro, 2018; Save the Children, 2019 como se citó en Orosco Fabian et al., 2022) y estos se han incrementado durante la pandemia por eso el ciberbullying se define como el acoso entre iguales dentro del contexto digital, en donde principalmente participan el acosador, la víctima y los espectadores, con la finalidad de afectar la dignidad personal y dañarlo socialmente en cuanto a los medios que se utilizan para este tipo de acoso están los mensajes por correo electrónico, mensajería instantánea, llamadas telefónicas y publicaciones en redes sociales de Facebook, Instagram y Tinder Y las formas de ciberacoso más comunes se dan a través de insultos, palabras ofensivas, memes, mensajes de voz con violencia verbal, distribución de vídeos furtivos, indiferencia en mensajería instantánea y en convivencia en WhatsApp (Orosco et al.,2022).

Caso en Guayaquil:

“Durante el mes de agosto, la Arcotel (Agencia de Regulación y Control de las Telecomunicaciones) hizo un llamado a los ciudadanos para que tengan precaución con su rastro digital, enfatizando que "la identidad es invaluable". Esta advertencia surgió después de que se realizara un proceso masivo de escaneo del iris a personas en las ciudades de Guayaquil y Quito, donde se ofrecía una compensación en monedas digitales a cambio de este procedimiento.

La Arcotel destacó la importancia de salvaguardar elementos como las características faciales y el iris ocular, ya que constituyen información biométrica que

podría ser aprovechada por delincuentes cibernéticos para sustraer datos personales".

2.2 Marco Legal:

2.2.1. La Constitución de la República 2008:

El Artículo 66 de la Constitución de Ecuador establece el reconocimiento y la garantía de los siguientes derechos fundamentales para las personas:

Numeral 19:

Derecho a la protección de información personales, el cual abarca la facultad de acceder y tomar decisiones sobre los datos personales, juntos con su debida protección. Cualquier actividad de recopilación, almacenamiento, tratamiento, distribución o divulgación de esta información personal requiere el consentimiento expreso de su propietario o debe estar respaldad por disposición legal.

Numeral 20:

Derecho a la privacidad en el ámbito personal y del núcleo familiar.

Numeral 21:

Derecho a la integridad y confidencialidad de las comunicaciones, tanto físicas como digitales. Estas comunicaciones no pueden ser interceptarles, abiertas o revisadas, salvo en situaciones específicamente contempladas por la ley, requiriendo autorización judicial previa y manteniendo la confidencialidad sobre temas no relacionados con el motivo de la revisión. Este derecho protege cualquier tipo o forma de comunicación. (Asamblea Nacional - Registro Oficial 449, 2008)

2.2.2. El Código Orgánico Integral Penal (COIP)

Artículo 178 - Violación a la intimidad:

Este artículo establece que cualquier persona que sin permiso o si respaldo legal acceda, capture, revise, conserve, registre, copie, comparta o haga público información privada de otra persona (como datos personales, mensajes, grabaciones de voz o video, correspondencia, archivos digitales o comunicaciones confidenciales) utilizando cualquier método, recibirá una condena de prisión entre uno y tres años. (Asamblea Nacional – Registro Oficial 180, 2014)

Artículo 186 – Estafa:

Este artículo define la estafa como el acto de una persona que busca obtener ganancias económicas para sí misma o para otros mediante el engaño. Esto incluye inventar situaciones falsas, distorsionar la realidad o esconder información verdadera para confundir a otra persona y hacer que tome decisiones que afecten negativamente su patrimonio o el de tercero. La sanción es prisión de cinco a siete años.

Se aplicará la pena máxima (siete años) cuando la estafa se cometa mediante:

1.El uso fraudulento de tarjetas bancarias (credito, debito o pago) que hayn sido modificados, copiadas ilegalmente, sustraidas o conseguidas sin el consentimiento del dueño legitimo.

2.El empleo de equipos electronicos que interfieran con cajeros automaticos para alteral, copiar o duplicar los dispositovs origianles, con el proposito de obtener y reporudcir informacion de tarjatas bancarias. (Asamblea Nacional – Registro Oficial 180, 2014)

Análisis

Los numerales 1 y 2 del artículo abordan directamente modalidades que son inherentes a la criminalidad cibernética moderna. El uso fraudulento de tarjetas de crédito, débito o pago cuando estas han sido “alteradas, clonadas. Duplicadas, hurtada, robada y obtenida sin legitimo consentimiento” describe perfectamente el modus operandi de muchos casos de suplantación de identidad digital, donde los delincuentes obtienen datos financieros a través de phishing, malware o ingeniería social.

La mención a dispositivos electrónicos que alteren modifique, clonen o dupliquen en el numeral dos reconoce el desarrollo tecnológico de estos delitos y la necesidad de tipificar específicamente el uso de herramientas digitales para la realización de defraudes.

Artículo 190 - Apropiación fraudulenta por medios electrónicos:

Este artículo sanciona a quien emplee de manera deshonesta sistema computacionales o redes de comunicación digital para apoderarse ilegalmente de

propiedades ajenas a realizar transferencias de bienes, valores o derechos sin autorización de propietario. La conducta incluye modificar, alterar o manipular el funcionamiento normal de redes digitales, software, sistemas computacionales y equipos de telecomunicaciones para beneficio propio de terceros. La penalidad establecida es de uno a tres años de prisión.

La misma pena se aplica cuando el delito se ejecuta mediante la desactivación de sistemas de seguridad o vigilancia, el descifrado de códigos secretos o encriptados, el uso no autorizado de tarjetas con banda magnética o perforadas, el empleo de dispositivos de control remoto para apertura, o la vulneración de medidas de seguridad electrónicos, informáticas o similares. (Asamblea Nacional – Registro Oficial 180, 2014)

Artículo 211 - Supresión, alteración o suposición de la identidad y estado civil:

Se penaliza a quien de forma ilegal obstaculice, modifique, agregue o elimine información de identidad (propia o ajena) en sistemas informáticos, documentos oficiales, tarjetas, índices, cedulas o cualquier otro documento expedido por el Registro Civil y sus oficinas. También se sanciona a quien registre falsamente como propio un hijo que no le pertenece. La pena establecida es de uno a tres años de pena privativa de libertad.

Sobre la Suplantación de identidad en su artículo 212:

Quien se haga pasar por otra persona con el fin de conseguir algún beneficio personal o para alguien más, causando daño a otra persona, recibirá una pena privativa de libertad entre uno y tres años.

Artículo 229:

Revelación ilegal de base de datos: Cualquier individuo que revele datos almacenados en archivos, registros, bases de datos o sistemas similares que funcione mediante plataformas electrónicas, informáticas o de telecomunicaciones, violando deliberadamente la confidencialidad y privacidad de las personas para beneficio propio o ajeno, será castigado con prisión de uno a tres años. Cuando esta acción se

cometida por funcionarios públicos, empleados de bancos o instituciones financieras de economía popular y solidaria, o su contratista, la pena se incrementa de tres a cincos de prisión. (Asamblea Nacional – Registro Oficial 180, 2014)

Artículo 230:

Interceptación ilegal de datos: Se impondrá pena de prisión de tres a cinco años a:

- Quien de manera ilicita cree, desarrolle, ejecute o envie contenido digital malicioso como codigos de acceso contraseñas, certificados de seguridad o paginas web falsas, ventanas emergentes o enlaces fraudulentos, o altere sistemas de nombres de dominio de servicios financieros o sitios de confianza, con el propósito de engañar a las personas para que ingresen a sitios web distintos a los que realmente desean visitar.
- Quien reproduzca, duplique o venda ilegalmente la información contenida en bandas magnéticas, chips u otros componentes electrónicos de tarjetas de crédito, débito, pago o similares, utilizando cualquier metodo disponible. (Asamblea Nacional – Registro Oficial 180, 2014)

Análisis

Phishing y sitios fraudulentos: Este numeral criminaliza específicamente una de las técnicas más utilizadas para la suplantación de identidad cibernética. El phishing mediante paginas falsas de servicios financieros o sitios de confianza representa el método principal para obtener credenciales de acceso que posteriormente se utilizan para suplantar la identidad digital de las víctimas. La modificación del sistema DNS constituye una forma sofisticada de redirigir hacia sitios controlados por atacantes.

Clonación de tarjetas: La reproducción de información de tarjetas bancarias facilita directamente la suplantación de identidad financiera, permitiendo a los delincuentes realizar transacciones haciéndose pasar por los legítimos portadores de las tarjetas.

Artículo 231:

Transferencia electrónica de activo patrimonial: Quien busque obtener ganancias económicas, mediante la alteración, manipulación o modificación de programas informáticos, sistemas telemáticos o mensajes digitales, con el propósito de conseguir sin autorización la transferencia o apropiación de bienes económicos de otra persona, causándole daño a terceros, recibirá una sanción de prisión de tres a cinco años. (Asamblea Nacional – Registro Oficial 180, 2014)

Art. 232:

Ataque a la integridad de sistemas informáticos. - Quien cause daño intencional a sistemas digitales, computadoras, redes de comunicación, equipos electrónicos o infraestructura tecnológicas ya sea destruyéndolos, alterándolos, bloqueándolos o interfiriendo con su funcionamiento de un sistema informático de manera ilegal, recibirá una condena de prisión de 3 a 5 años.

Delitos contra la información pública reservada legalmente. – La misma sanción penal se aplicará a quien cree, desarrolle, programe, compre, envié, instale, ejecute, comercialice o distribuya por cualquier software malicioso, programas dañinos o sistemas informáticos diseñados específicamente para provocar los daños dichos anteriormente.

Cuando estos delitos informaticos se comentan contra sistemas que prestan servicios publicos o que estan relacionados con la seguridad pública, la pena se incirmenta a un rango de 5 a 7 años de prisión preventiva. (Asamblea Nacional – Registro Oficial 180, 2014)

Art. 233:

Se aplicará la misma penalización legal a cualquier persona que diseñe, elabore, codifique, adquiera, transmita, implemente, active, venda difunda cualquier tipo de software malintencionado, aplicaciones nocivas o sistemas computacionales creados expresamente para causar los perjuicios mencionados anteriormente. (Asamblea Nacional – Registro Oficial 180, 2014)

Art. 234:

Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. -

1.Quien ingrese sin permiso a un sistema informático telemático, ya sea completamente o parcialmente, o permanezca en el sin consentimiento del propietario legítimo, recibirá prisión preventiva de tres a cinco años.

2. Si la persona accede ilegalmente al sistema con el propósito de aprovecharse indebidamente de dicho acceso, alterar sitios web, desviar el flujo de información o comunicaciones, o brindar a terceros los servicios que proporcionan estos sistemas sin compensar a los proveedores legítimos, será condenado con prisión preventiva de tres a cinco años. (Asamblea Nacional – Registro Oficial 180, 2014)

2.2.3. La Ley Orgánica de Protección de Datos Personales

En su artículo 1 señala el objeto y la finalidad que busca salvaguardar la información personal, lo cual abarca el acceso y control sobre la información y datos, junto con su respectiva seguridad. Con este propósito, establece, contempla y elabora fundamentos, derechos, deberes y sistemas de amparo. (Asamblea Nacional - Registro Oficial 459, 2021)

El Artículo 4 sobre los términos y definiciones donde el organismo autónomo es responsable de vigilar el cumplimiento de esta normativa, su implementación y las decisiones que emita, con la finalidad de proteger los derechos y libertades esenciales de las personas en relación con el manejo de su información personal.

Dato biométrico: Es la información personal que refiere a rasgos físicos, fisiológicos o comportamiento de una persona que posibilita o verifica su identificaron exclusiva, incluyendo fotografías del rostro o registros de huellas dactilares, entre otros.

Dato genético: Vinculada con particularidades genéticas hereditarias o desarrolladas por una persona, que aportar datos únicos sobre su constitución física o estado de salud.

Dato personal: Permite identificar o busca hacer reconocible a una persona de manera directa o indirecta.

Datos personales crediticios: Datos que integran el comportamiento económico de personas naturales, para evaluar su solvencia financiera. (Asamblea Nacional - Registro Oficial 459, 2021)

Art. 10.- Principios:

Sin perjuicio de otros que están en la Constitución de la República, los instrumentos internacionales verificados por el Estado u otras normas jurídicas, la presente Ley se regirá por:

g) Confidencialidad. El tratamiento de datos personales debe garantizar la confidencialidad y el secreto. No deben ser tratados ni compartidos con ningún fin distinto al de su recopilación, salvo que existan motivos válidos que permitan su posterior tratamiento en las condiciones legítimas establecidas en esta Ley.

j) Seguridad de los datos personales. Los responsables del tratamiento de datos personales deben implementar todas las medidas de seguridad necesarias. Estas medidas, que pueden ser organizativas, técnicas o de otro tipo, deben proteger los datos personales de cualquier riesgo, amenaza o vulnerabilidad. Esta protección debe considerar la naturaleza de los datos personales, así como su alcance y contexto. (Asamblea Nacional - Registro Oficial 459, 2021)

Art. 11.- Normativa especializada:

Los datos personales que se traten bajo normas especiales relacionadas con la libertad de expresión, sectores regulados específicos, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado, así como los datos personales que deban entregarse a autoridades administrativas o judiciales en cumplimiento de solicitudes y órdenes con base en la legislación vigente, se ajustarán a los principios establecidos en su normativa específica y a los principios establecidos en esta Ley, cuando corresponda. En todos los casos, deberán observarse los estándares internacionales de derechos humanos y los principios de esta Ley, junto con los criterios mínimos de legalidad, proporcionalidad y necesidad. (Asamblea Nacional - Registro Oficial 459, 2021)

Art. 23.- Derecho a la educación digital:

Las personas tienen derecho a acceder al conocimiento, el aprendizaje, la preparación, el estudio, la formación, la enseñanza y la instrucción relacionados con el uso y la gestión adecuados, saludables, constructivos, seguros y responsables de las tecnologías de la información y la comunicación. Esto debe respetar los principios de dignidad e integridad humanas, así como los derechos fundamentales y las libertades individuales. Se debe prestar especial atención a la privacidad, la vida personal, la capacidad de controlar la propia información, la identidad y reputación en línea, la ciudadanía digital y el derecho a la protección de datos personales. Además, existe el derecho a fomentar una cultura que valore la protección de datos personales. El derecho a la educación digital será inclusivo, en particular para las personas con necesidades educativas especiales. El sistema educativo nacional, incluida la educación superior, garantizará la educación digital para estudiantes de todos los niveles y para el profesorado. El profesorado debe incluir este tema en sus procesos de formación. (Asamblea Nacional - Registro Oficial 459, 2021)

El derecho a la educación digital garantiza que las personas adquieran no solo habilidades tecnológicas, sino también competencias críticas, éticas y sociales que les permitan desenvolverse en un mundo digitalizado, protegiendo sus derechos y ejerciendo plenamente su ciudadanía en línea.

Art. 37.- Seguridad de datos personales:

La seguridad de los datos personales no solo es un requisito técnico, sino un derecho humano y un deber social. Garantizarla implica proteger la libertad individual y fortalecer la confianza en los entornos digitales.

El responsable o encargado del tratamiento de datos personales, según corresponda, deberá adherirse al principio de seguridad de los datos personales, para lo cual deberá considerar las categorías y el volumen de datos personales, el estado de la técnica, las mejores prácticas de seguridad integral y los costos de aplicación según la naturaleza, el alcance, el contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos. El responsable o encargado del tratamiento de datos personales deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas técnicas, organizativas y de cualquier otra índole implementadas para

garantizar y mejorar la seguridad del tratamiento de datos personales. El responsable del tratamiento de datos personales deberá demostrar que ha adoptado medidas que reduzcan significativamente los riesgos detectados. Otros aspectos podrían ser similares:

1) Medidas encaminadas a mantener la confidencialidad, integridad y disponibilidad permanente de los sistemas y servicios de procesamiento de datos personales, así como el acceso rápido a los datos personales en caso de incidentes; y

2) Medidas encaminadas a mejorar la resiliencia técnica, física, administrativa y jurídica.

3) Los responsables y encargados del procesamiento de datos personales podrán adherirse a estándares internacionales para la gestión adecuada de riesgos enfocada en la protección de derechos y libertades, así como para la implementación y gestión de sistemas de seguridad de la información o códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales. (Asamblea Nacional - Registro Oficial 459, 2021)

- Se establecen principios técnicos esenciales (confidencialidad, integridad, disponibilidad).
- Se exige una resiliencia integral que abarque lo técnico, físico, administrativo y jurídico.
- Se promueve la adhesión a estándares internacionales y marcos normativos que garanticen una gestión responsable y con alcance global.

Art. 43.- Notificación de vulneración de seguridad:

La notificación de vulneración de seguridad es un mecanismo que protege a los ciudadanos y refuerza la confianza en la gestión de datos personales. No se limita a cumplir con un trámite legal, sino que busca minimizar el impacto del incidente, garantizar la rendición de cuentas de las organizaciones y proteger la dignidad, privacidad y derechos digitales de las personas.

El responsable del tratamiento de datos deberá notificar a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las

Telecomunicaciones cualquier violación de datos personales lo antes posible y, en todo caso, en un plazo máximo de cinco (5) días desde su conocimiento, salvo que sea improbable que dicha violación constituya un riesgo para los derechos y libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no se produce en un plazo de cinco (5) días, deberá ir acompañada de una indicación de los motivos de la demora. El encargado del tratamiento de datos deberá notificar al responsable cualquier violación de datos personales lo antes posible y, en todo caso, en un plazo máximo de dos (2) días desde su conocimiento. (Asamblea Nacional - Registro Oficial 459, 2021)

Art. 45:

Garantía del secreto de las comunicaciones y seguridad de datos personales. - Los proveedores de servicios de telecomunicaciones deben garantizar el secreto de las comunicaciones y la seguridad de los datos personales para la correcta prestación de los servicios de telecomunicaciones y el correcto funcionamiento de las redes de telecomunicaciones. Los equipos, la infraestructura y las instalaciones que permiten la grabación del contenido de determinadas comunicaciones, ordenadas por los tribunales competentes, solo podrán ser utilizados por los proveedores de servicios de telecomunicaciones por orden judicial. Las disposiciones de esta Ley serán aplicables si se prueba la grabación o interceptación no autorizada de las comunicaciones. (Asamblea Nacional - Registro Oficial 459, 2021)

2.2.4. Tratados o Convenios Internacionales

Convenio sobre la Ciberdelincuencia o Convenio de Budapest

Artículo 2- Acceso ilícito:

Los países adoptarán las medidas legislativas y demás disposiciones que resulten necesarias para considerar como conducta criminal en su derecho interno el acceso deliberado e ilegítimo a la totalidad de un sistema informático. Los Estados podrán establecer que el delito que se cometa infringiendo medidas de seguridad, con la intención de conseguir datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otros objetos de sistema informático. (Consejo de Europa, 2001)

Análisis

"Enfatiza la necesidad de que los países criminalicen el acceso no autorizado a sistemas informáticos. La intención es que las legislaciones internas consideren un delito el acceso deliberado e ilegítimo a la totalidad de un sistema informático. Además, se faculta a los Estados para que también penalicen las intrusiones que se realicen infringiendo medidas de seguridad con el propósito de obtener datos o con cualquier otra intención delictiva, especialmente cuando el sistema informático está conectado a otros sistemas, lo que subraya la gravedad de este tipo de crímenes en un mundo interconectado".

Artículo 7- Falsificación informática:

Los países que participan deberán implementar las medidas legislativas y regulaciones que resulten necesarias para considerar como delito la modificación ilegal de información digital. Esto incluye cuando una persona deliberadamente introduzca, altere, borre o elimine datos informáticos con el propósito de crear información falsa que genere datos no auténticos que sean tomados o utilizados a efecto legales como auténticos, con independencia de que los datos sean legibles e inteligentes directamente. Los países tienen la opción de exigir que exista una intención dolosa o delictiva similar para que se pueda establecer que existe responsabilidad penal. (Consejo de Europa, 2001, p.6)

Su control depende tanto de la legislación vigente como de la implementación de buenas prácticas tecnológicas y culturales en el manejo de datos.

2.2.5La Declaración Universal de los Derechos Humanos

Art.6

Toda persona tiene derecho, al reconocimiento de su personalidad jurídica en cualquier lugar del mundo. (Asamblea General de las Naciones Unidas, 1948, p3)

El derecho al reconocimiento de la personalidad jurídica es un pilar de la igualdad y la protección de derechos humanos, asegurando que cada individuo sea considerado sujeto de derechos en cualquier lugar del mundo y pueda participar plenamente en la vida legal, social y digital.

Art. 12

Ninguna persona será objeto de injerencias arbitrarias en su intimidad personal, en su núcleo familia, su hogar o su correspondencia privada, ni de ataques a su dignidad o a su buen nombre. Cualquier persona tiene derecho de ser amparado por la ley que protege contra este tipo de intromisión o arrebatos. (Asamblea General de las Naciones Unidas, 1948, p.4)

Análisis

"La suplantación de identidad no aparece nombrada en la DUDH, pero se desprende de la protección de la identidad, la personalidad jurídica, la privacidad y la honra, recogidas principalmente en los artículos 6 y 12".

Tabla 1. Legislación Comparada

Conducta penalizada	Argentina	Colombia	Brasil	México
Norma legal que tipifica los delitos informáticos	Código Penal, Art. 153, Art. 125, Art. 145 bis, Art. 183.	Código Penal, Arts.192-197	Código Penal, Art. 154-A	Códigos Penal Federal, Art. 211 bis 1
Conductas tipificadas	violación de correspondencia digital; acceso ilegítimo a datos o a sistema informático; publicación ilegal o abusiva de comunicación electrónica; revelación de secretos oficiales; acceso	Esta ley sanciona el delito de corrupción, también contempla la violación de correspondencia o comunicaciones, violación de datos personales, extorsión, estafa	Invadir un dispositivo informático utilizado por otra persona, esté o no conectado a una red informática, con el fin de obtener, manipular o destruir datos o información sin	Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos

	ilegítimo, difusión o alteración de datos personales; estafa o fraude informático; daño en datos y sistemas informáticos; interrupción o entorpecimiento de comunicaciones electrónicas; y alteración de medios probatorios.	informática, daño informático, espionaje, sabotaje informático, suplantación de identidad, espionaje informático, instalación o propagación de programas informáticos maliciosos, suplantación de páginas electrónicas, facilitación de delito informático y difusión de información falsa	la autorización expresa o tácita del usuario del dispositivo, o instalar vulnerabilidades para obtener una ventaja ilícita, la misma pena se aplica a quien produzca, ofrezca, distribuya, venda o difunda un dispositivo o programa informático con la intención de posibilitar la práctica de la conducta definida en el caput.	por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de

				prisión y de cincuenta a ciento cincuenta días multa.

Elaborado por: Cordova y Moreno (2025)

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Enfoque de la investigación:

La orientación de esta investigación es de carácter cualitativo para abordar el fenómeno de la suplantación de identidad y su impacto en la seguridad digital, representa una perspectiva metodológica fundamental para comprender fenómenos complejos desde la experiencia, percepciones que los individuos atribuyen a sus vivencias.

La investigación Cualitativa se centra en comprender y profundizar los fenómenos, analizándolos desde el punto de vista de los participantes en su ambiente y en relación con los aspectos que los rodean. Normalmente es escogido cuando se busca comprender la perspectiva de individuos o grupos de personas a los que se investigará, acerca de los sucesos que los rodean, ahondar en sus experiencias, opiniones, conociendo de esta forma cómo subjetivamente perciben su realidad (Guerrero, 2016, p.3).

3.2 Alcance de la investigación:

En la investigación con alcance descriptivo de tipo cualitativo, se busca realizar estudios de tipo fenomenológicos o narrativos constructivistas, que busquen describir las representaciones subjetivas que emergen en un grupo humano sobre un determinado fenómeno (Galarza, 2020, pp 1-6).

El alcance metodológico de este enfoque investigativo se orienta hacia la respuesta de interrogantes fundamentales relacionadas con el que, como, cuando, donde, quien. Utilizando métodos como la observación, entrevistas a profundidad o el análisis de documentos para capturar la riqueza de las experiencias y los significados que los participantes le dan a sus realidades.

Esta delimitación conceptual no debe interpretar como una limitación, sino como una especialización metodológica que permite la obtención de descripciones precisas, detalladas y sistemáticas observada.

3.3 Técnica e instrumentos para obtener los datos

Según Diaz Bravo (2013), indica que:

La entrevista es una técnica de gran utilidad en la investigación cualitativa para recabar datos; se define como una conversación que se propone un fin determinado distinto al simple hecho de conversar. Es un instrumento técnico que adopta la forma de un diálogo coloquial. Canales la define como "la comunicación interpersonal establecida entre el investigador y el sujeto de estudio, a fin de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto". Se argumenta que la entrevista es más eficaz que el cuestionario porque obtiene información más completa y profunda, además presenta la posibilidad de aclarar dudas durante el proceso, asegurando respuestas más útiles (pp. 162-167).

Según (Folgueiras,2016) una entrevista busca recopilar dicha información que se genera en un margen sistematizado, mediante el uso de esta estrategia se concede llevar un proceso de investigación ya sea de manera oral o personalizada por medio de una estructura que jerarquice por medio del entrevistado y el entrevistador.

Al mencionar el instrumento de entrevista permite tener un contacto directo con nuestros profesionales en el tema, conocer las perspectivas de los principales factores que conllevan a la suplantación de identidad. El instrumento de esta entrevista fue implementada a través de un cuestionario compuesto por ocho preguntas para abordar las dimensiones más relevantes del fenómeno bajo investigación.

Tabla 2.Temas para tratar durante las entrevistas

Conceptualización personal	¿Podría explicarnos, en sus palabras, qué es la suplantación de identidad en el entorno digital?
Estrategias y metodologías	¿Cuáles son los métodos más frecuentes que utilizan los delincuentes para obtener datos personales?
Impacto	¿Qué consecuencias puede tener la suplantación de identidad para la víctima?

Estrategias preventivas	Desde su experiencia, ¿qué medidas preventivas puede tomar una persona para proteger su identidad en línea?
Acciones que se recomienda	¿Qué acciones recomendaría tomar inmediatamente si alguien sospecha que su identidad ha sido suplantada?
Compromiso y Responsabilidad	¿Considera que las empresas y plataformas digitales están haciendo lo suficiente para proteger los datos personales de sus usuarios?
Análisis crítico acerca de políticas educativas	¿Cree usted que debería incluirse la educación sobre seguridad digital y suplantación de identidad en las escuelas?
Percepción de la evolución del fenómeno	En un contexto cada vez más digitalizado, ¿considera que este problema va en aumento?

Elaborado por: Cordova y Moreno (2025)

3.4 Población y muestra

La muestra de esta investigación emplea un enfoque no probabilístico por criterio de expertos debido a que busca obtener información rica y detallada sobre el fenómeno de estudio de la suplantación de identidad cibernética. Las entrevistas realizadas a expertos en el tema de la seguridad cibernética que conlleva a la suplantación de identidad de los diferentes afectados. Este proceso de análisis permite conocer a detalle cómo reaccionar ante estos casos de delito cibernético. Cada entrevistado tiene el conocimiento y experiencia de solventar las diferentes dudas y propuestas para mejorar en dichos casos.

La población elegida está conformada por personas que han sido víctimas o han estado cerca de este tipo de delito en cual se muestra como han evolucionado de manera directa e indirecta este fenómeno digital, se fundamenta en el hecho de que cualquier individuo u organización que mantenga presencia digital está potencialmente expuesto a riesgos de suplantación de identidad, independientemente

de su nivel de conocimiento tecnológico o las medidas de seguridad que se implemente.

Mediante la entrevista que está constituida por profesionales con experiencia, investigación y persecución de este tipo de delitos, garantizando así la obtención de información técnica especializada sobre esta problemática. De igual manera, mostrando las diferentes formas de caer en una estafa virtual con sus respectivas consecuencias, alternativas de cómo evitar ser estafados mediante las diferentes redes sociales, plataformas digitales u otros.

CAPÍTULO IV

PROPUESTA O INFORME

4.1 Presentación y análisis de resultados

4.1.1 Entrevistas

Tabla 3**.** Entrevista al Abogado Jaime Lenin Hurtado Angulo

Nombre del Abogado Experto: Abogado Jaime Lenin Hurtado Angulo	Magíster en Derecho Procesal Master en Protección de Datos PhD. Ciencias Jurídicas (propiedad intelectual)	
Conceptualización personal	Pregunta: ¿Podría explicarnos, en sus palabras, qué es la suplantación de identidad en el entorno digital?	El termino phishing, tal como se denomina en la doctrina penal y en el ámbito de la informática, se relaciona estrechamente con la suplantación de identidad, concepto que también está reflejado en nuestra legislación, específicamente en el Código de ética internacional artículo 212. Este fenómeno consiste en asumir la identidad de otra persona con el objeto de obtener un beneficio personal o para una tercera persona. Actualmente, este delito es especialmente frecuente en los entornos

		digitales, generalmente, los usuarios interactúan a través de computadoras, tabletas o teléfonos inteligentes, dispositivos que suelen estar protegidos por sistemas de seguridad que, en ocasiones, incluyen la presencia de las llamadas cookies. Estas cookies, en el mejor de los casos, funcionan como mecanismo de recopilación de información hábitos de navegación en el mejor escenario. Sin embargo, en ciertos casos, las cookies pueden no ser inocuas pues sirven para obtener credenciales tales como nombre de usuario y contraseñas de diversas plataformas. Al obtener esta información, los delincuentes pueden asumir la identidad del usuario en dichas plataformas y utilizarla con fines que consideren convenientes.
Estrategias y metodologías	Pregunta: ¿Cuáles son los métodos más frecuentes que utilizan los delincuentes para obtener datos personales?	En el ámbito de las redes sociales, existe una falta generaliza de conocimiento sobre los riesgos que implican la exposición de información personal en estas plataformas. Por ejemplo, muchos usuarios de Facebook no configuran adecuadamente las opciones de privacidad, permitiendo que si información sea accesible públicamente en lugar de restringir el acceso únicamente a alas personas seleccionadas.

		Esta situación representa un riesgo considerable, ya que la información personal puede ser utilizada de manera fraudulenta, incluso llegando a la suplantación de identidad dentro de dicha red social. De manera similar, en el comercio electrónico pueden presentarse situaciones de riesgo. Por ejemplo, algunas personas acceden a páginas que aparentan ser seguras, como temu, una plataforma de comercio electrónico popular en la actualidad. Sin embargo, existen sitios fraudulentos que imitan la apariencia de esta página legitimas, con el fin de obtener información personal, claves de acceso e incluso datos financieros de los usuarios. Una vez que los delincuentes obtienen estas credenciales, pueden asumir la identidad digital de la víctima y acceder a su patrimonio.

Impacto	Pregunta: ¿Qué consecuencias puede tener la suplantación de identidad para la víctima?	Bueno hay diversas consecuencias dependiendo de la circunstancia. Se trata de la información financiera, obviamente el perjuicio patrimonial. Si se trata de información personal, esa información personal puede ser utilizada contra la víctima, es decir, por ejemplo, asumo la identidad de una persona determinada y habiéndolo hecho me contacto con otra que me cae mal, y la insulto en los peores términos entonces ahí las consecuencias. Y ahora no es un problema eso, con la inteligencia artificial, ¿verdad?, asumo y ahogo de todo y hasta que yo me parezca a una equis persona, pues las consecuencias pueden ser muy nocivas para la victima de suplantación de identidad. Entonces, son dependiendo de las circunstancias serán más o menos profundas las consecuencias para la víctima de suplantación de identidad.
Estrategias preventivas	Pregunta: Desde su experiencia, ¿qué medidas preventivas puede tomar una persona para proteger su identidad en línea?	Es importante, primero que sepamos que cuando accedemos a una plataforma red social, es gratuita, no nos cuesta darnos de alta en Facebook o en Instagram o ninguna red social cobra por la creación de una cuenta. Pero en internet nada es gratis. Cuando dicen que no nos cobran es porque nuestra información personal es la moneda de cambio, donde nos

		piden nuestros nombres dirección, correo electrónico y donde tienen, acceso a nuestra dirección IP. Y luego nos piden información de terceros ya que, al poner fotografías de nuestro núcleo familiar, entonces toda esa información es con lo que pagamos a este servicio que nos dan las redes sociales. Entonces, teniendo conocimiento de eso, podremos evitar dar más allá de la información estrictamente necesaria para el manejo de la red social. Con frecuencia debemos cambiar nuestras claves de acceso para evitar que personas que deambulan en el entorno digital no puedan deducir con facilidad o encontrarse por accidente o intencionalmente en nuestra identidad digital se utilizarla indebidamente. Estas son medidas de seguridad, pero partiendo de nuestros derechos como titulares de datos personales tenemos la Ley Orgánica de Datos Personales está vigente desde el 2021 en el Ecuador. Y hay una superintendencia de protección de datos personales que hay un reglamento de la Ley de Protección de Datos Personales. Es decir, todo un sistema de protección de datos personales que antes del 2021 lo teníamos. Conociendo de esta ley, del sistema de protección y datos, tendremos mayor

		conciencia lo que debemos y lo que no debemos o no podemos hacer en entornos digitales para precautelar nuestros derechos y libertades como titulares de los datos personales. En todo ámbito ya sea familiar, profesional, financiero, necesitamos tener plena conciencia de los riesgos que asumimos cuando lo hacemos de forma tan inadvertida y de por supuesto que las plataformas también tienen su parte. En protección de datos hay un principio que se llama protección de datos desde el diseño y por defecto. ¿Qué quiere decir eso? Que los proveedores de estos servicios de redes sociales como Facebook están obligados a configurar sus plataformas para que aseguren a los usuarios el mayor nivel de seguridad posible, aun cuando el usuario no tenga conocimientos suficientes para modificar o ajustar dichas configuraciones. Esto es un tema que ya la ley de protección de datos exige y no solamente la ley de nuestro país, sino la legislación internacional de forma unánime exige en las plataformas la protección de datos desde el diseño y por defecto, justamente porque muchos de los usuarios no tienen conciencia de lo que pueden hacer para proteger su información personal.

Acciones que se recomienda	Pregunta: ¿Qué acciones recomendaría tomar inmediatamente si alguien sospecha que su identidad ha sido suplantada?	Primero la inmediata modificación de las credenciales, de claves, usuarios, de inmediatamente el bloqueo, esto constituye la medida inicial más efectiva. Posteriormente si tenemos claridad de lo que ha ocurrido, se debe acudir y promover la denuncia, la policía judicial dispone de una división de informática forense conformada por peritos informáticos que pueden eventualmente detectar el origen de los delitos. Estas medidas deben adoptarse independientemente del cambio inicial de credenciales, con el fin de prevenir la continuidad de la afectación debemos permitir que las autoridades realicen la investigación adecuada del caso
Compromiso y Responsabilidad	Pregunta: ¿Considera que las empresas y plataformas digitales están haciendo lo suficiente para proteger los datos personales de sus usuarios?	Actualmente no lo están haciendo, es una tarea pendiente, incluso en la superintendencia de protección de datos personales, está empeñada en ello. Existe una figura en el sistema de protección de datos del país que es el delegado de Protección de Datos Personales, este profesional está destinado o tiene la tarea de asesorar tanto a los que procesan datos personales, o a los encargados de tratamiento de datos personales, que son aquellos que procesan datos personales, por cuenta de los responsables y que los asesoran para la aplicación correcta de

		las normas de la ley de protección orgánica de protección de datos personales. Asesoran a los titulares de los datos personales de la mejor manera de ejercer sus derechos, derechos de acceso, derechos de rectificación, derechos de su respuesta, derechos de oposición, derechos de portabilidad. Esos derechos que tenemos como usuario y como titular de datos personales el delegado de protección de datos personales nos asesora sobre la forma en que tenemos que ejercerlos ante el responsable. Ese responsable no actúa como dice la ley, ese delegado de protección de datos puede también coordinar los generales de derechos pueden ejercer tales derechos ante la autoridad de control de protección de datos. Esto es la superintendencia de protección de datos. Nos va a permitir que el sistema de protección de datos en el país se desarrolle adecuadamente, como dice la ley, como dice la legislación internacional, sobre todo en la europea, la cual ha servido como referente para la elaboración de nuestra ley nacional.
Análisis crítico acerca de políticas educativas	¿Cree usted que debería incluirse la educación sobre seguridad	Sí, mientras más sepamos, menos expuesto estaremos a la vulneración de nuestros datos personales.

	digital y suplantación de identidad en las escuelas?	Los menores de edad son nativos digitales como se les denomina, han nacido y crecido los entornos digitales. A diferencia para la generación del siglo pasado, para quienes el acceso a estas herramientas era ilimitado. En la medida que sepan los riesgos que corren, que sepan que no pueden confiar en la gente, los peligros que ellos corren son aún más graves que los que corremos las mayores edades. Recordemos el acoso cibernético, el sexting, la pornografía infantil son delitos que ponen en riesgo la indemnidad, incluso psicológica y sexual en los menores de edad. Los menores de edad pueden dar su consentimiento para recopilar sus datos personales en el Ecuador a partir de los 15 años. Pero incluso a esta edad, muchos adolescentes puede que no estén consientes de los peligros. Pero en la medida que conozcan, que se enseñe, que se advierta, esos riesgos serán atenuados y sus derechos serán preservados. Eso le corresponde, por supuesto, a todos, a la autoridad de protección de datos, a los colegios, las escuelas que los docentes tengan estén capacitados pueden transmitirlo a sus estudiantes, a los padres de familia, que sepan que deben tener, controles parentales, en las tablets, computadoras,

		teléfonos inteligentes que usan los jóvenes, los niños, para evitar justamente exponerlos a esos peligros.
Percepción de la evolución del fenómeno	Pregunta: En un contexto cada vez más digitalizado, ¿considera que este problema va en aumento?	Sí, aumenta exponencialmente. Porque primero en países en vía de desarrollo como el Ecuador, aún la riqueza digital es muy marcada. Parece que entre los que tienen acceso a las tecnologías de la información y la comunicación, que tienen el conocimiento para su manejo y de los que no tienen ni siquiera la energía eléctrica en sus barrios, en sus casas. Esa brecha está cerrándose cada vez más. Personas expuestas a los riesgos de estas tecnologías y la falta de conocimiento hace que también aumente las víctimas potenciales de infracciones. Entonces, es tarea de la autoridad de protección de datos personales inicialmente educar a la población, sobre los riesgos, sobre nuestros derechos, las formas de ejercerlos que los que manejan datos personales, me refiero, por ejemplo, a los dueños de almacenes y directores de establecimientos educativos de todo nivel. A los dueños de grandes corporaciones o los negocios pequeños, cómo deben manejar los datos personales propios, de sus colaboradores, de sus clientes Todos estamos involucrados en el sistema de protección de datos. Todos procesamos datos en una mayor o menor medida, en casa procesamos datos no solamente nuestra familia, más cercana, sino nuestros familiares y amigos. En una fiesta, una reunión familiar, llegan familiares y amigos, tomamos fotos y los subimos a redes sociales. Estamos manejando datos personales de esas personas y las estamos exponiendo en las redes sociales.

Elaborado por: Cordova y Moreno (2025)

Tabla 4. Entrevista de la Jueza Andrea Moreno Silva

Nombre del Abogado Experto: Andrea Moreno Silva	Jueza Penal - Unidad Judicial Penal Norte 2	
Conceptualización personal	Pregunta: ¿Podría explicarnos, en sus palabras, ¿qué es la suplantación de identidad en el entorno digital?	Es cuando una persona se hace pasar por otra, ya sea ya sea por Chats o ahora que está la inteligencia artificial y también por voz que te realizan llamadas engañando por ejemplo que necesita cierta recompensa porque se encuentra en un accidente, o llame con porque necesita dinero por alguna situación, así se puede dar la suplantación de la persona es decir que simule ser otra persona o con el fin de sacar algún rédito económico o estafar a la gente.
Estrategias y metodología	Pregunta: ¿Cuáles son los métodos más frecuentes que utilizan los delincuentes para obtener datos personales?	Considero que lo más común en la actualidad vienen a ser los datos obtenidos a través de redes sociales, a través de información que se tiene registrada en la base de datos de los bancos.

		Es por ello que esta información muchas veces recae de empleados bancarios que justamente manejan información de las personas que tienen registradas sus cuentas en una entidad bancaria. Entonces, para ellos es más factible a través de estos medios electrónicos, a través de estas redes de información obtener datos personales de cada víctima que en este caso se va a eliminar algún tipo de infracción. Y eso deja abierto muchas posibilidades de ingresar y obtener información.

Impacto	Pregunta: ¿Qué consecuencias puede tener la suplantación de identidad para la víctima?	De los casos que conozco, la suplantación muchas veces conlleva a que se utilicen estos datos, sobre todo cédulas falsas para que, a través de esta información, delinquir, obtener préstamos, inclusive préstamos que la persona nunca ha realizado y con una ligereza muchas veces de la entidad que van a proporcionar un crédito y de alguna manera manipulan esta información. He visto víctimas que están afectadas con préstamos que nunca han realizado en valores altos. Así también los hacen partícipes como que han cometido algún tipo de infracción, obviamente utilizando la cédula, por ejemplo, en una compraventa ficticia, en una compraventa de algún bien, hacen aparentar que compró en tal fecha y luego que esa persona le vendió a otra, para hacer una triangulación y puede de alguna manera tener información, y hacer contratos ilícitos.

Estrategias preventivas	Pregunta: Desde su experiencia, ¿qué medidas preventivas puede tomar una persona para proteger su identidad en línea?	Bueno realmente sí se nota un poco complejo porque ya hay cierta información personal que ya es pública. Entonces, sí se torna un poco complejo que la gente u otras personas, en este caso delincuentes, accedan a una información de datos, quizás como una medida de protección de poder no tener redes abiertas, sino más bien restringidas. Cuanto al banco pues contar con un personal idóneo, en este caso que va ser la persona que va a estar cuidando las cuentas. Esto más que nada lo digo porque siempre ocurre que se dan por la información de la persona, hacen transferencias que no han sido autorizadas o en este caso valores económicos que no han sido autorizados por la cuenta ahorrista. Yo creía que una oficial de crédito idónea tiene que velar también por aquello. Ver que, si hay un movimiento inusual en la cuenta de una persona, se alerte para que no haya este riesgo de que se le están apropiando de sus valores. Como primer acto de seguridad, las cuentas, las redes sociales no estén abiertas de libre acceso, siendo bastante restringida y lo que compete a instituciones bancarias, que estas tengan un personal idóneo, en este

		caso, oficiales de crédito que vean movimientos inusuales y sepan advertir al cliente que está ocurriendo cierta situación.
Acciones que se recomienda	Pregunta: ¿Qué acciones recomendaría tomar inmediatamente si alguien sospecha que su identidad ha sido suplantada?	Presentar una denuncia ante la fiscalía, para que esta institución como titular de la acción penal pública pueda realizar ya los fallos urgentes para evitar que en este caso trascienda algún acto de la falsificación de identidad, pero lastimosamente estas causas se ven cuando ya ha sido ciertamente consumada, no se puede advertir que va a ocurrir y que le han suplantado a esta persona. Cuando el hecho ya está Lo que debe hacer la víctima porque es tratar es inmediatamente tratar de presentar la denuncia en la fiscalía para que se realicen las investigaciones pertinentes. Por ejemplo, una persona le suplantaron la identidad, hicieron un préstamo, un contrato de que adquiría algún equipo electrodoméstico, muchas veces cuando se entera la persona de que ha sido suplantada su identidad es cuando ya le están haciendo los cobros en las instituciones.

		Entonces, ahí recién se moviliza la persona para saber qué es lo que pasó. Pero hay que saber que efectivamente dentro de la investigación que realiza la fiscalía se puede dar con estas personas, quién suplantó y qué situación realizó, qué acto ilícito realizó. Presentar la denuncia es lo que correspondería.
Compromiso y Responsabilidad	Pregunta: ¿Considera que las empresas y plataformas digitales están haciendo lo suficiente para proteger los datos personales de sus usuarios?	Por los casos que se han visto considero que no, que hay gente infiltrada lastimosamente, hay funcionarios buenos, funcionarios malos y pues no todos ellos van a tener sentido de cuidado por el bien del otro, sino que también, lastimosamente se prestan porque hay una vulnerabilidad en cuanto al tema de redes, al tema electrónico, muchas veces son objetos hasta de hackeos, Entonces es muy complicado, pero que haya una correcta seguridad dentro de una institución en cuanto a los datos de las personas la veo bastante vulnerable, no está al 100% segura.
Análisis crítico acerca de políticas educativas	¿Cree usted que debería incluirse la educación sobre seguridad digital y	Desde luego que sí, que se cree una cultura de precaución, porque no solamente los datos los adquieren a través de las personas adultas, sino

	suplantación de identidad en las escuelas?	también de las personas menores de edad, cuyos padres manejan cuentas y van obteniendo esa información que para ellos es válida para saber los movimientos, estilo de vida de cada persona e ir a un blanco perfecto para el momento de delinquir. Entonces crearse una cultura de seguridad en cuanto a esta información personal que tiene cada cuenta, cada persona.
Percepción de la evolución del fenómeno	Pregunta: En un contexto cada vez más digitalizado, ¿considera que este problema va en aumento?	He visto casos, sí, pero no como que sea un tipo de delito de mayor incidencia. Ciertamente está ligado a que de alguna manera van tener información de los datos de una persona como para cometer delitos de extorsión, pero sería como extenderme demasiado entre una cosa y otra, pues estamos hablando de protección de datos personales, pero si bien es cierto que hoy en día el auge de los delitos que se están cometiendo a diario es el delito de secuestro, secuestro extorsivo, intimidación, sí debe existir una restricción, un cuidado, porque de la mano esta situación, no te van a estar suplantando la identidad o un delito prioritario pero de alguna manera obtener datos de una persona sí está involucrando a que te puedan ser objeto de otro tipo de delitos, como por ejemplo de mayor gravedad, un delito de extorsión,

		Porque saben tus datos, saben por dónde vives, entonces si bien es cierto no te están suplantando la identidad, pero a través de ellos obtienen datos de esta persona. Reitero, no es un delito de suplantación, es más un delito de auge o un delito de mayor incidencia en nuestra sociedad, pero si hay casos en los que normalmente la suplantación es utilizada para contratos ilegítimos, crear préstamos que no han sido, en este caso, solicitados por la víctima, compra de electrodomésticos, cuestiones así, que sí les afecta en la economía.

Elaborado por: Cordova y Moreno (2025)

Tabla 5. Entrevista del Fiscal Marco Ordeñana Baldeón

Nombre del Abogado Experto: Marco Ordeñana Baldeón	Fiscal Provincial de los Ríos. Docente Universitario de las Universidades Unemi y Ecotec a nivel de Pregrado y Posgrado	
Conceptualización personal	Pregunta: ¿Podría explicarnos, en sus palabras, ¿qué es la suplantación de identidad en el entorno digital?	En términos generales, la suplantación de identidad es cuando una persona realiza acciones para hacerse pasar por otra persona con el propósito de ejecutar ciertos actos ilícitos como por ejemplo realizar créditos o cualquier otra actividad ilegal. En el plano digital entonces esa acción de suplantar la identidad de otra persona también se ejecuta a través de medios digitales como por ejemplo cuando una persona se crea un perfil falso en una red social también con el propósito de denigrar aquella persona por la que se está haciendo pasar o para incurrir en la comisión de actividades ilícitas.
Estrategias y metodologías	Pregunta: ¿Cuáles son los métodos más frecuentes que	En el plano normal, lo que hacía una persona para hacerse pasar por otra, precisamente era la de tomar sus

	utilizan los delincuentes para obtener datos personales?	datos personales, como por ejemplo una cédula, ¿no? Le sacaba la foto y colocaba en la cédula entidad la foto del suplantador. Como ahora la sociedad ha evolucionado hacia un entorno digital, por lo tanto también se incurren en este tipo de actos obviamente en este medio, siendo las formas más conocidas, por ejemplo la que se conoce como el nombre de phishing, que es a través de la utilización de correos falsos con los cuales se puede acceder a datos de otras personas, o también lo que se conoce como el nombre de smishing, que significa los mensajes de texto, cuando se los envían a otra persona a través de esta modalidad con el propósito de tener información, o también lo que se conoce con el nombre de vishing, son llamadas telefónicas, como por ejemplo cuando una persona que se hace pasar como empleado de banco, es tanto su poder de convencimiento que logra simplemente a través de llamadas obtener datos personales de otras personas como sus direcciones domiciliarias, correos electrónicos, o incluso no solamente el número normal de la tarjeta de crédito, sino el código secreto con el cual

		posteriormente adquieren compra. También hay una modalidad que se conoce con el nombre de malware, que está relacionado con los programas maliciosos, o también los spyware, que es relacionado con el robo de contraseñas, cuando por ejemplo le envían un correo electrónico y le dicen que le van a eliminar su cuenta de email, porque no ha actualizado los datos en el que se pide contraseña y la gente inocente incurre o cae en este tipo de engaños y cede y da sus datos personales, incluidas sus contraseñas de los correos electrónicos, también hay una forma común de su creación de identidad a través de los medios digitales como es la creación de páginas falsas que es una de las más conocidas a través por ejemplo de la cual Pedro toma fotografías o adquiere fotografías de Juan y se crea un perfil de Juan cuando es Pedro el que está interactuando en forma maliciosa a través de esa red social en perjuicio, perdón, de quien se ha suplantado. También hay formas de ingeniería social que es justamente la manipulación psicológica de las víctimas como por ejemplo cuando llaman y le dicen que ha recibido una

		inconveniente de una persona o que está detenido, un pariente y la persona sin ver al supuesto pariente comienza a proporcionar sus datos personales para ayudarlos. Obviamente hay otra forma de adquirir datos personales a través de las redes públicas de Wifi por ejemplo porque estas son totalmente vulnerables a los sistemas de seguridad cuando una persona deja su computador o deja su teléfono, no tiene servicio internet, entonces decide enlazarse como una red social pública y eso es una de las modas más fáciles de poder sustraer la información y finalmente podríamos decir las propias redes sociales cuando las personas sin que siquiera se lo pida a otro por su propia cuenta publican sus datos personales, por ejemplo en una página de Facebook como la dirección de su domicilio como sus números telefónicos e incluso algunos ponen ingenuamente hasta sus números celulares, por lo cual aquello constituye una forma muy fácil de que extraños que se mueven tras la sombra de una situación digital pueden hacer esta información y utilizarla en hechos electivos.

Impacto	Pregunta: ¿Qué consecuencias puede tener la suplantación de identidad para la víctima?	La víctima definitivamente puede tener una arista de consecuencias que van a afectar a sus intereses estas pueden ser por ejemplo de naturaleza económica ya que en el momento que le suplantan su identidad, por ejemplo, a través de la adquisición de datos de su tarjeta de crédito, la van a endeudar, ¿no? Es en haber adquirido un producto que ha ido al destino o a las manos perniciosas de quienes incurrieron en este tipo de normalidad, esta persona que resulta ser víctima de este hecho obviamente va a tener conflicto económico por cuanto va a verse obligada a cubrir deuda de las que ella no adquirió o incluso podría terminar con impedimentos legales para adquirir créditos como por ejemplo cuando la registran en el buró de créditos por mora por deudas que ella no adquirido. Las consecuencias también pueden ser legales porque se pueden cometer delitos en nombre de esta persona como por ejemplo, estafas, adquisición de objetos a través del engaño con los cuales obviamente la persona suplantada no tiene ningún tipo de relación pero como son sus nombres, sus datos son los que constan, la persona perjudicada por

		dirigir su carga jurídica contra la persona cuya identidad es la que cuenta en los registros de adquisición de bienes por lo tanto también podría tener consecuencias no solamente económica sino también penales que incluso pueden desencadenar en penas de prisión preventiva. Otra de las consecuencias también es la reputación de la persona, por ejemplo una de las modalidades más frecuentes era la creación de páginas falsas y hay muchas personas que suplantan la identidad de otra y ofrecen hasta servicios sexuales entonces el quien se enganchan con esa red de piensan que esta persona que es víctima de una suplantación de identidad por medio digitales está ofreciendo servicios sexuales y por lo tanto su reputación se va a ver totalmente afectada por este tipo de conductas obviamente que también la pérdida de privacidad va a ser determinante en este tipo de situaciones porque sus datos van a quedar expuestos al público y finalmente el impacto emocional psicológico obviamente va a padecer la víctima en este tipo de situaciones va padecer una carga emocional totalmente negativa que

		ha desencadenado que muchas ocasiones la víctima en estos casos incluso incurra al suicidio porque no soportan el tipo de perjuicio que están padeciendo como consecuencia de la suplantación de su persona a través de medios digitales, nosotros vemos que el tema de la suplantación de identidad no solamente afecta a personas ingenuas, Otra de las consecuencias también es la reputación de la persona porque por ejemplo hace un momento le dice que una de las modalidades más frecuentes era la creación de páginas falsas y hay muchas personas que suplantan la identidad de otra y ofrecen hasta servicios sexuales entonces quien se engancha con esas redes piensa que esta personas que es víctima de una suplantación de identidad por medio digitales está ofreciendo servicios sexuales y por lo tanto su reputación se va a ver totalmente afectada por este tipo de conductas obviamente que también la pérdida de privacidad va a ser determinante en este tipo de situaciones porque sus datos van a quedar expuestos al público y finalmente el impacto emocional psicológico obviamente va a padecer la víctima en este tipo

		de situaciones no va a padecer la víctima o una carga emocional totalmente negativa que ha desencadenado que muchas ocasiones la víctima en estos casos incluso incurran al suicidio porque no soportan el tipo de perjuicio que están padeciendo como consecuencia de la suplantación de su personas a través de medios digitales
Estrategias preventivas	Pregunta: Desde su experiencia, ¿qué medidas preventivas puede tomar una persona para proteger su identidad en línea?	La víctima definitivamente puede tener una arista de consecuencias que van a afectar a sus intereses estas pueden ser por ejemplo de naturaleza económica ya que en el momento que le suplantan su identidad, por ejemplo, a través de la adquisición de datos de su tarjeta de crédito, la van a endeudar, ¿no? Es en haber adquirido un producto que ha ido al destino o a las manos perniciosas de quienes incurrieron en este tipo de normalidad, esta persona que resulta ser víctima de este hecho obviamente va a tener conflicto económico por cuanto va a verse obligada a cubrir deuda de las que ella no adquirió o incluso podría terminar con impedimentos legales para adquirir créditos como por

		ejemplo cuando la registran en el buró de crédito por mora por deudas que ella no adquirido. Las consecuencias también pueden ser legales porque se pueden cometer delitos en nombre de esta persona como por ejemplo, estafas, adquisición de objetos a través del engaño con los cuales obviamente la persona suplantada no tiene ningún tipo de relación pero como son sus nombres, sus datos son los que constan, la persona perjudicada por dirigir su carga jurídica contra la persona cuya identidad es la que cuenta en los registros de adquisición de bienes por lo tanto también podría tener consecuencias no solamente económica sino también penales que incluso pueden desencadenar en penas de prisión preventiva. Otra de las consecuencias también es la reputación de la persona, por ejemplo una de las modalidades más frecuentes era la creación de páginas falsas y hay muchas personas que suplantan la identidad de otra y ofrecen hasta servicios sexuales entonces el quien se enganchan con esa red de piensan que esta persona que es víctima de una suplantación de identidad por

		medio digitales está ofreciendo servicios sexuales y por lo tanto su reputación se va a ver totalmente afectada por este tipo de conductas obviamente que también la pérdida de privacidad va a ser determinante en este tipo de situaciones porque sus datos van a quedar expuestos al público y finalmente el impacto emocional psicológico obviamente va a padecer la víctima en este tipo de situaciones va padecer una carga emocional totalmente negativa que ha desencadenado que muchas ocasiones la víctima en estos casos incluso incurra al suicidio porque no soportan el tipo de perjuicio que están padeciendo como consecuencia de la suplantación de su persona a través de medios digitales, nosotros vemos que el tema de la suplantación de identidad no solamente afecta a personas ingenuas, Otra de las consecuencias también es la reputación de la persona porque por ejemplo hace un momento le dice que una de las modalidades más frecuentes era la creación de páginas falsas y hay muchas personas que suplantan la identidad de otra y ofrecen hasta servicios sexuales entonces el quien se venganza con esa red piensa que

		esta personas que es víctima de una suplantación de identidad por medio digitales está ofreciendo servicios sexuales y por lo tanto su reputación se va a ver totalmente afectada por este tipo de conductas obviamente que también la pérdida de privacidad va a ser determinante en este tipo de situaciones porque sus datos van a quedar expuestos al público y finalmente el impacto emocional psicológico obviamente va a padecer la víctima en este tipo de situaciones no va a padecer la víctima o una carga emocional totalmente negativa que ha desencadenado que muchas ocasiones la víctima en estos casos incluso incurran al suicidio porque no soportan el tipo de perjuicio que están padeciendo como consecuencia de la suplantación de su personas a través de medios digitales

Acciones que se recomienda	Pregunta: ¿Qué acciones recomendaría tomar inmediatamente si alguien sospecha que su identidad ha sido suplantada?	Nosotros vemos que el tema de la suplantación de identidad no solamente afecta a personas ingenuas o personas confiadas, sino también a personas que son desconfiadas de profesionales, incluso a gente que sabe sobre estas cosas. Obviamente que, en un mayor margen, las personas que desconocen sobre la utilización de la plataforma son las que son más víctimas de este tipo de suplicación de identidad, por lo tanto, colateralmente de otros eventos delictivos, sin embargo, las medidas que se podrían aplicarse, ya por ejemplo, que se utilicen contraseñas seguras y únicas. Por ejemplo, hay personas que tienen Instagram, Facebook, o tienen tres o cuatro y hasta cinco correos electrónicos, y a los cinco o cuatro correos electrónicos le ponen la misma contraseña, o a todas las redes sociales le ponen la misma contraseña. Y no solamente eso, sino que además le ponen contraseñas fáciles, como, por ejemplo, sus propias fechas de nacimiento o la fecha de nacimiento de sus hijos, de sus padres. Entonces, los delincuentes digitales, lo primero que comienzan a sondear

		respecto a las contraseñas justamente a través de la fecha de su nacimiento que es dicho sea de paso, están expuestas en la propia red social. Entonces, ¿que hace el delincuente? Sin necesidad de haber hecho alguna actividad de demasiado esfuerzo intelectual sino simplemente por lógica. Toma la fecha de nacimiento, lo diga la contraseña y pueden acceder a sus redes sociales. Por lo tanto, una de las medidas justamente no utilizar la misma contraseña en varias redes sociales y que las mismas sean contraseñas seguras. Es decir, contraseñas combinadas a través de números, a través de letras y también de otra figura ortográfica como, por ejemplo, asteriscos numerales, letras mayúsculas, letras minúsculas. Es decir, hay que combinar las contraseñas para hacerlas bastante es compleja. Hay que tener también definitivamente privacidad en redes sociales porque de por sí las redes sociales son públicas, pero igual podemos restringirlas para que puedan hacer a las mismas solamente en nuestros contactos. El problema es que la gente la deja abierta y por lo tanto gente extraña, gente desconocida,

		tiene acceso a las mismas y por lo tanto puede tener acceso a sus datos consecuentemente la persona que expone sus redes sociales en forma pública es mucho más vulnerable que aquella que las utiliza en forma privada. Evitar, hace un momento les dije que una de las formas más usuales de robar la información es cuando uno se conecta a una red de WIFI pública. Por lo tanto, el consejo es que no utilicen este tipo de accesos para poder conectarse hacia las plataformas digitales, no creer esos enlaces y correos sospechosos cuando le dicen te vamos a cerrar tu cuenta de correo, te vamos a cerrar tu cuenta de Facebook, el banco va a cerrar tu cuenta porque tienes que actualizar la información y la gente ingenuamente actualiza la información. Por lo tanto, esto es una de las formas más utilizadas por los delincuentes cibernéticos con el propósito de acceder a la información personal de las personas. Otra modalidad también sería revisar frecuentemente sus redes sociales, las personas muchas veces tienen redes sociales y la revisan cada dos semanas, cada mes y por lo tanto no se percatan de

		que a través de una cuenta donde le han suplantado la identidad, por ejemplo están pidiendo colaboración económica o prestar sus redes sociales a su contacto justamente de las redes sociales y una de las situaciones más importantes la educación digital, nosotros permitimos que nuestros hijos desde muy pequeños tengan redes sociales, Facebook, internet, etcétera, pero el problema es que no le educamos en el ámbito digital de cómo deben de actuar frente a posibles ataques cibernéticos a posibles hechos delictivos y esto es como cuando una persona adulta no sabe leer ni escribir, es decir una persona analfabeta en el ámbito de la lectura también podemos llevarlo eso al ámbito digital, es decir una persona que no sabe manejar la informática consecuentemente aunque sepa leer y escribir termina constituyéndose en un analfabeto digital porque no sabe el manejo de las redes sociales y por lo tanto la mejor forma de prevenir los ataques cibernéticos entre los cuales se encuentra la sustracción de la identidad personal de quienes hacen uso de las redes sociales justamente a través de la educación digital..

Compromiso y Responsabilidad	Pregunta: ¿Considera que las empresas y plataformas digitales están haciendo lo suficiente para proteger los datos personales de sus usuarios?	La información o la sustracción de los datos personales de las personas no se produce solamente con un ataque cibernético dirigido a un individuo, sino que también se pueden producir con ataques dirigidos a empresas. Porque normalmente las empresas cuentan con datos conjuntos de individuos, por ejemplo, todos sus trabajadores, entonces al delincuente digital se le hace más beneficioso atacar a una empresa donde puede a la vez sustraer, los datos personales de 200 personas a la vez y no hacerlo una por una porque va a demandar mucho más tiempo. Por lo tanto, nosotros vemos el tema de las estafas a través del uso de empresas falsas o incluso la transferencia dolosa de dinero a través de una cuenta a otra bancaria, o las compras a través de tarjetas de crédito. Entonces si bien es cierto que muchas veces estas actividades ilícitas se producen por ingenuidad de los usuarios, en un gran porcentaje también se producen precisamente por la vulneración de los sistemas informáticos de las instituciones tanto de las empresas como de las entidades bancarias. Por lo tanto, es evidente que los

		sistemas informáticos de estas compañías y de las bancarias son totalmente frágiles y vulnerables para la delincuencia cibernética.
Análisis crítico acerca de políticas educativas	¿Cree usted que debería incluirse la educación sobre seguridad digital y suplantación de identidad en las escuelas?	Una de las formas de prevenir es justamente la educación desde el aspecto informático y por lo tanto hablando del aspecto informático está incluido el tema relacionado con la suplantación de identidad o la suplantación de datos personales que podrían conllevar a la comisión de otros delitos y meter en graves problemas a aquella persona que siendo víctima de una suplantación de identidad digital además tiene que enfrentar problemas legales, económicos y de otra naturaleza. Por lo tanto, si estamos hablando que por el solo hecho de no saber leer ni escribir a una persona se le denomina analfabeta. Entonces a una persona por el hecho de no saber manejar el tema de la informática debe denominarse un analfabeto del aspecto informático, es decir un analfabeto moderno. Por lo tanto, para evitar eso el Estado debe establecer una política educativa encaminada no solamente a enseñar a leer y a escribir a las personas sino manejar el tema de las redes sociales, el tema de la

		informática. Porque en definitiva la sociedad ha dejado ya de realizar sus actividades en el plano físico en un gran porcentaje para ir hacia los medios digitales y por lo tanto la educación debe de centrarse en este último sentido.
Percepción de la evolución del fenómeno	Pregunta: En un contexto cada vez más digitalizado, ¿considera que este problema va en aumento?	Nosotros bastamos leer los medios de comunicación como diarios y las propias redes sociales para percatarnos que cada vez existen más víctimas en el plano digital de sustracción de datos personales, de sustracción de identidad y de otras infracciones. Y cuando nosotros vamos a la fiscalía y levantamos una estadística vemos que los hechos delictivos en el plano digital están también en aumento y que incluso hay cierto tipo de conductas delictivas como por ejemplo las estafas o las transferencias de dineros a través de medios ilegales que han superado a las que se cometen en el lugar de los hechos físicos y que ahora se cometen a través de los medios digitales. Por lo tanto, hay cierto tipo de delitos que cometiéndose en el mundo digital han superado en número a aquellos que se cometen en el mundo físico.

		Es evidentemente que este tipo de conductas han trascendido al mundo no físico y se encuentran en aumento.

Elaborado por: Córdova y Moreno (2025)

4.1.2 Análisis global de las entrevistas

Los entrevistados, expertos en el tema abogados, evidencian cuales son los factores transcendentales que conllevan a la suplantación de identidad por medio de la cibernética, por lo tanto, una de ellas son el uso de las redes sociales colocando información relevante en su perfil, el poco conocimiento de aceptar cualquiera cookie sin leer las advertencias se convierte en un escenario fácil de caer para robar datos importantes de los usuarios.

Dentro del banco de preguntas, que se le realizo a los diferentes especialistas concuerdan que por medio de los diferentes sitios web son el principal factor que conlleva al delito cibernético. Añadiendo, que las redes sociales son el eje principal para obtener información como nombres, dirección de domicilio, edad, medios de contacto u otros, cada experto menciona la importancia de mantener cierta información de manera privada para evitar caer en estafas, suplantación de identidad y otras actividades que conllevan a poner en peligro nuestra privacidad.

Cabe mencionar, que la abogada Andrea Moreno hace hincapié que cierta información que se consideraba personal ya es publica por los diferentes medios del estado, por ejemplo, al acceder buscar una persona por medio del registro civil mediante el sitio web es factible, al igual que buscar una persona que este demandado y otros casos que son de manera pública.

En efecto, la poca importancia que cada usuario sube a su red social o plataforma digital sin ninguna responsabilidad genera los diferentes ataques cibernéticos y llegan a ser un objetivo fácil para el estafador cibernético. Al igual como se mencionó, el analfabetismo digital se convierte en el problema mayor de la población no tener una orientación o conocimiento adecuado sobre las causas y consecuencias de no saber usar, manejar los diferentes sitios web, plataformas digitales y redes sociales.

Es fundamental conocer nuestros derechos como ciudadanos que nos ampara la Ley de Protección de datos personales, por medio de los diferentes profesionales en la rama que nos asesoran para usarlo de una manera adecuada y responsable. El abogado Jaime Hurtado, menciona la importancia de tener una educación sobre temas de la seguridad digital y suplantación de identidad en las aulas de clases, el

cual incluye un conocimiento amplio sobre las diferentes formas de ser estafados y evitar los riesgos que implican.

Hacer uso de las diferentes redes sociales no implica peligro si tiene un uso adecuado, es necesario que cada usuario conozca las ventajas y desventajas al hacer uso de los diferentes sitios web, permitirá evitar caer en los diferentes métodos de ser estafado, suplantar su identidad u obtener información personal que comprometa al individuo.

Sin embargo, la nueva era digital ha evolucionado de una manera brusca donde la generación antigua busca adaptarse de una forma que no se vea afecta o cometan errores que les generen consecuencias graves, a pesar, que ciertos grupos de personas ya han sido víctimas de los ataques cibernéticos que se presentan en las diferentes plataformas digitales.

4.2 Propuesta

En esta investigación se realizó un estudio detallado que permitió conocer sobre la suplantación de identidad y el ataque cibernético que cada usuario sin tener un conocimiento previo se ve afectado por las diferentes técnicas de estafas. La siguiente propuesta busca generar una seguridad digital por medio de un proceso educativo, por ende, las diferentes técnicas y mecanismos que utilizan los estafadores cibernéticos.

Es importante mencionar, los diferentes actores involucrados que conllevan a los casos de los ciberdelincuentes que son el eje principal de la suplantación de identidad sus diversas técnicas que usan para lograr obtener información personal o incluso corporativas. Al igual que los diferentes servicios digitales que se ofrecen en las plataformas y redes sociales, no llevar un control adecuado sobre la información que se emite se enfrentan a un desafío difícil de manejar, principalmente a la ausencia de profesionales capacitados en temas de ciberseguridad.

En efecto, a pesar de los incomparables casos de ataques cibernéticos o suplantación de identidad se debe crear estrategias de prevención y mitigación que se basen en tecnologías que sean emergentes y busquen marcos regulatorios. De tal manera, sustentar esta problemática es crear soluciones que sean viables dentro de las diferentes normas legislativas, el cual se plantean propuestas que prioricen temas

de educación y analfabetismo digital con las diversas regulaciones legales para proteger la identidad de cada ciudadano.

4.2.1.Creación de normativa clara y precisa

Tal como lo menciona el (Asamblea Nacional – Registro Oficial 180, 2014). “las mismas penas se impondrán al, que, sin estar autorizado, se apodere, utilice o modifique en perjuicio de tercero, datos reservados de carácter personal o familiar…” (Art. 197.2).

Hace referencia al apoderamiento sin autorización de datos que son reservados en los diferentes sitios web, una persona que realice un ataque cibernético acoge toda la información de los usuarios que sin conocimiento previo ingresan datos importantes. Cabe mencionar que esta ley sanciona a quienes hacen uso o difusión no autorizada por el propietario, pero no ejerce el rol de trabajar de una manera directa en mejoras para evitar suplantaciones de identidad.

Implementar normas en beneficio de la persona afectada permitirá salvaguardar y reparar a las víctimas, al igual que obtener el apoyo de los diferentes países desarrollará un ambiente de prevención y protección de la identidad digital.

4.2.2.Implementar programas educativos de alfabetismo digital

El desarrollo de iniciativas formativas enfocadas en competencias digitales representa un mecanismo de prevención esencial para disminuir la exposición a riesgos de usurpación de identidad en línea, dotando a las personas de las habilidades indispensables para desenvolverse con seguridad en el ecosistema digital contemporáneo.

La creación de programas de capacitación en habilidades digitales configura una medida preventiva crucial para minimizar la susceptibilidad frente a ataques de falsificación de identidad digital, brindando a los ciudadanos las destrezas requeridas para interactuar de forma protegida en plataformas y servicios online.

El establecimiento de cursos educativos orientados al dominio de tecnologías digitales constituye una táctica de protección primaria para reducir la vulnerabilidad contra fraudes de suplantación identitaria cibernética, ofreciendo a los individuos las capacidades fundamentales para operar con prudencia en espacios virtuales.

Los diferentes centros de educación se han ido acoplando a la nueva era digital impartiendo clases sobre la inteligencia artificial el uso de redes y cómo mejorar, con el objetivo principal que las nuevas generaciones se adapten al nuevo mundo virtual obteniendo resultados favorables. Cabe mencionar, que existe un alto índice de personas que aún se enfrenta a los cambios bruscos del uso de la tecnología, el cual son las principales víctimas de los ciberdelincuentes.

Es vital crear, materiales educativos que se centren en ciertos grupos determinados como las simulaciones de ataque virtual, los riesgos de una suplantación de identidad, conocer los intentos de phishing y las varias amenazas que se enfrentan en el ámbito tecnológico.

4.2.3.Mejorar mecanismos de protección y recuperación de identidad

Fortalecer los mecanismos de protección y recuperación de identidad para las víctimas implica desarrollar acciones y recursos que resguarden la privacidad, dignidad y derechos de personas que sufrieron apropiación indebida de su identidad. Incluye protocolos de atención urgente, apoyo legal y psicológico, además de procesos expeditos para restaurar la identidad y reparar daños. Es crucial garantizar la protección de la intimidad durante todo el proceso, evitar la revictimización y mantener la confidencialidad.

Se requieren canales de denuncia seguros y cooperación interinstitucional para facilitar la recuperación y prevenir riesgos futuros. Mejorar estos sistemas protege a las víctimas y fortalece la confianza en las instituciones, promoviendo respuestas integrales ante delitos identitarios

El poco conocimiento que se tiene sobre la suplantación de identidad o ataques de robo de datos personales en un grupo determinado genera los diversos problemas sociales que se enfrenta a diario. En ciertas ocasiones, estas organizaciones que se dedican al robo de información se encuentran aliadas a ciertas empresas o plataformas digitales, es por ello, que tener derecho a los daños ocasionadas por terceras personas debe ser prioritario, al igual que los diferentes procesos de judiciales sean agiles dentro de los diferentes centros administrativos.

Existe un alto índice de ineficiencia en temas de modelos legislativos como la falta de reglamentación en ciertas zonas determinadas, la poca capacitación que

tienen ciertas autoridades. Es vital mantener un mecanismo de protección al momento de la recuperación de identidad de los afectados.

Los distintos modelos que manejan otros países debe ser una guía para nuestro sector, como la Unión Europea maneja los diferentes reglamentos de protección de datos creando seguridad y confianza en las diferentes transacciones o movimientos electrónicos.

CONCLUSIONES

●El análisis de las diferentes modalidades de suplantar la identidad cibernética o ser estafados por las diferentes plataformas digitales, redes sociales y sitios web se ha convertido en la actualidad una problemática para los diferentes usuarios que navegan en el internet, sin tener alguna precaución de las consecuencias que se genere en el momento. Las varias formas de ser víctimas de estos delitos se generan a través de los correos electrónicos que llegan a las bandejas de los usuarios, las estafas por el WhatsApp, las cookies recolectan información importante de nuestros datos personales.

●Ecuador es un país que se encuentra en una severa amenaza constante a los diferentes ataques cibernéticos, es por ello, que los cambios bruscos que se han ido enfrentando como la adaptación de nuevas tecnologías son el causante principal para ser víctimas de estafas, suplantaciones de identidad y robo de información personal. Por ende, la falta de sensibilidad en los centros educativos se convierte en un causante de analfabetismo digital, y, los varios vacíos normativos generan un desafío dentro de las instituciones jurídicas mantener una actualización legislativa que generen respuestas integrales u acorde a las diversas necesidades de cada individuo.

●Dentro de la propuesta planteada busca conocer los factores principales que conllevan a caer de una manera fácil y directa en las diferentes modalidades de ser víctimas de estafas. Las diversas estrategias o alternativas permiten priorizar temas del analfabetismo digitales, prevención de mitigaciones y buscar soluciones que sean adaptables dentro de un determinado grupo. Lograr crear normativas que busquen amparar a los afectados devolviéndoles la confianza y firmeza que la nueva era digital conlleva sus ventajas y desventajas.

RECOMENDACIONES

- Cada usuario debe conocer a la problemática que se enfrente al momento de visitar un sitio web, redes sociales o plataformas digitales. Por otro lado, conocer la Ley de Código Orgánico Penal que ampara sobre este tipo de delitos cibernéticos es primordial para evitar cometer errores, al igual que priorizar la educación digital debe ser la base que toda institución educativa debe fomentar.

- Implementar estrategias que sirven para evitar el robo o suplantación de identidad y cuidar de nuestra seguridad cibernética, entre ellas tenemos la educación digital que permite conocer los riesgos que se enfrentan de hacer un uso indebido de los diferentes sitios web. Cada individuo debe informarse sobre las consecuencias de robar datos personales o usar la imagen de una tercera persona sin el consentimiento de esta, las diferentes campañas y normativas reconocen mejorar la seguridad de información personal que se suben a diario en las diferentes plataformas.

- Buscar alternativas fuera del país, también nos permite tener un amplio foro de ideas que fortalezcan las diferentes capacidades tanto técnicas y legales. Para ello, debe coexistir profesionales o expertos que guíen a la ciudadanía a no ser vulnerables ante las diversas maneras de ser engañados por terceras personas.

REFERENCIAS BIBLIOGRÁFICAS

Acevedo, E. Q. (2017). Revista jurídica. Investigación En Ciencias jurídicas Y Sociales. Obtenido de https://ojs.ministeriopublico.gov.py/index.php/rjmp/article/view/7/6

Albarran Martinez, E. E. (22 de Junio de 2021). REVISTATRANSREGIONES. Obtenido de https://revistatransregiones.com/web/index.php/tr/article/view/18/15

Alvarez, F. (2020). *DIALNET*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7763844

Asamblea General de las Naciones Unidas. (10 de Diciembre de 1948). *La Declaración Universal de los Derechos Humanos.* Obtenido de https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf

Asamblea Nacional – Registro Oficial 180. (2014 de Febrero de 2014). Código Orgánico Integral Penal. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Asamblea Nacional - Registro Oficial 449. (20 de Octubre de 2008). Constitución de la República del Ecuador. 40. Montecristi. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Asamblea Nacional - Registro Oficial 459. (26 de Mayo de 2021). Ley Orgánica de Protección de Datos Personales. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Benavides, E. F.-A. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia Y Tecnología, 13(1)*, 97-104. doi:https://doi.org/10.18779/cyt.v13i1.357

Código Orgánico Integral Penal . (10 de Febrero de 2014). *Registro Oficial Suplemento 180* . Obtenido de blob:https://app.lexis.com.ec/c902932f-92f2-48b4-8a8d-67f41e1ab978

Consejo de Europa. (23 de Noviembre de 2001). *Convenio sobre la Ciberdelincuencia o Convenio de Budapest*. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Daniel Orlando Icaza Álvarez, G. E. (2020). *El analfabetismo tecnológico o digital.* DIALNET.

Datareportal. (3 de Marzo de 2025). Obtenido de https://datareportal.com/reports/digital-2025-ecuador

De Aplicación Docente, D.D. (8 de Agosto de 2024). *Estafas Telefónicas y por WhatsApp: Cómo se Hacen y Consejos para Evitarlas*. Obtenido de DAD Departamento de Aplicación Docente: https://dad.uncuyo.edu.ar/estafas-telefonicas-y-por-whatsapp#:~:text=Estafas%20por%20WhatsApp:%20*%20Secuestro%20de%20Cuenta:,malware%20o%20redirigen%20a%20sitios%20de%20phishing.

Díaz Bravo, L. T. (2013). La entrevista, recurso flexible y dinámico. *Scielo*, 162-167. Obtenido de Investigación en educación médica: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-50572013000300009#:~:text=La%20entrevista%20es%20una%20t%C3%A9cnica,al%20simple%20hecho%20de%20conversar.&text=Es%20un%20instrumento%20t%C3%A9cnico%20que%20adopta%20la%20forma%20de%20un%20d

Díaz, F. (junio de 2024). Obtenido de https://repository.universidadean.edu.co/server/api/core/bitstreams/ae5f2c06-d7ce-4d0f-bbcc-81c271d8e65e/content

Echeburúa y De Corral . (2010). Adicción a las nuevas tecnologías y a las redes sociales en. Obtenido de https://www.redalyc.org/pdf/2891/289122889001.pdf

El Oriente. (24 de Junio de 2025). *El Oriente*. Obtenido de https://www.eloriente.com/articulo/las-estafas-digitales-aumentan-en-ecuador/51444

Fabian, J. R. (21 de Febrero de 2022). *Revista de Investigación Apuntes Universitarios*. Obtenido de https://d1wqtxts1xzle7.cloudfront.net/112595649/902-libre.pdf?1710954986=&response-content-disposition=inline%3B+filename%3DCiberbullying_en_estudiantes_desde_el_pe.pdf&Expires=1754171709&Signature=ZP1wQqkZkX7hnqQammHFZdYLawZF4xgd7jkYHlFfPx1Vr-Gnxq73dl5g6

Fernández Bermejo, D. ,. (09 de Noviembre de 2020). e-spacio.uned. *1*. Ediciones Experiencia. Obtenido de https://e-spacio.uned.es/entities/publication/87c43146-55ea-4d23-a74f-c614ae3430dc

Fernando Juca Maldonado, R. M. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas.

Folgueiras Bertomeu, P. (2016). La entrevista. Obtenido de https://diposit.ub.edu/dspace/bitstream/2445/99003/1/entrevista%20pf.pdf

Galarza, C. R. (2020). LOS ALCANCES DE UNA INVESTIGACIÓN. 5. doi:10.33210/ca.v9i3.336.

Guerrero Bejarano, M. (15 de Enero de 2016). Obtenido de http://201.159.222.115/index.php/innova/article/view/7/8

Herrera de las Heras, P. (2017). Responsabilidad civil por vulneración del derecho al honor en las redes sociales. 124. Madrid. Obtenido de https://www.torrossa.com/it/resources/an/4399537

Jimenez, R. (22 de Abril de 2024). *El Comercio* . Obtenido de Lo que debes saber sobre las ‘cookies’ de Internet : https://www.elcomercio.com/tecnologia/cookies-web-internet-informatica/

Machado, J. (10 de Junio de 2024). *Primicias*. Obtenido de https://www.primicias.ec/noticias/seguridad/ciberdelitos-ecuador-estafas-analfabetos-digitales-vulnerables/

Macías Lara, R. A. (2024). Estrategias innovadoras para mitigar la suplantación de identidad en redes sociales. *Revista Científica Multidisciplinar G-Nerando*. doi:https://doi.org/10.60100/rcmg.v5i1.212

Macías Lara, R. B. (30 de junio de 2024). Estrategias innovadoras para mitigar la suplantación de identidad en redes sociales. *5(1)*. Revista Científica Multidisciplinar G-Nerando. Obtenido de https://revista.gnerando.org/revista/index.php/RCMG/article/view/212/195

Ministerio de Gobierno. (04 de Agosto de 2025). *Las redes sociales son un 'arma' utilizada por estructuras dedicadas a la trata de personas*. Obtenido de Ministerio de Gobierno : https://www.ministeriodegobierno.gob.ec/las-redes-sociales-son-un-arma-utilizada-por-estructuras-dedicadas-a-la-trata-de-personas/#

Orosco Fabian, J. G. (21 de Febrero de 2022). *Ciberbullying en estudiantes desde el perfil de víctima en.* Obtenido de https://d1wqtxts1xzle7.cloudfront.net/112595649/902-libre.pdf?1710954986=&response-content-disposition=inline%3B+filename%3DCiberbullying_en_estudiantes_desde_el_pe.pdf&Expires=1754703620&Signature=O62tMpJQ28qA3HW9-vSeztYZbkaZ4Zwsm4Psxel79hdSbr~dIP1Wtvkdg

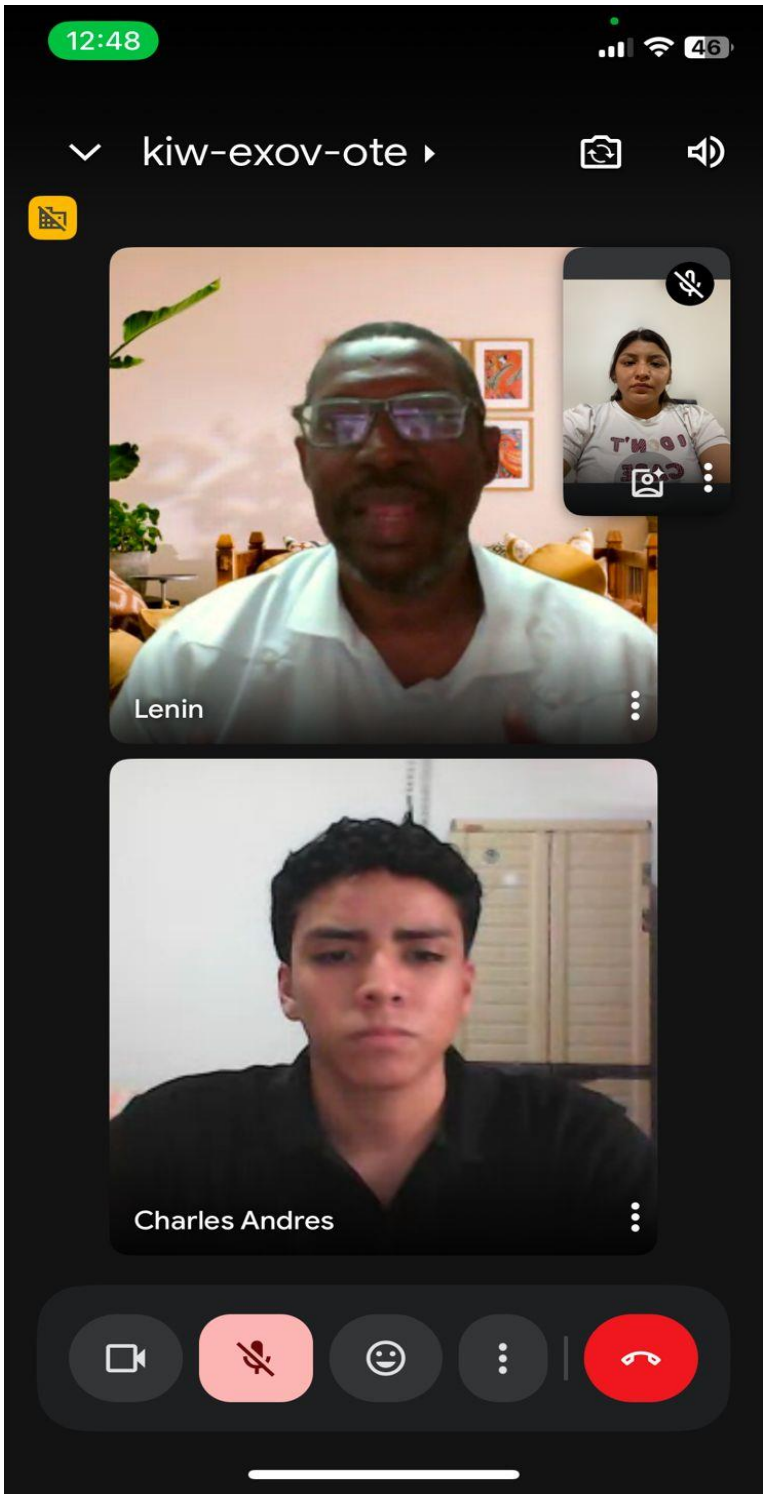
Redacción Banco Pichincha . (1 de Agosto de 2022). *Banco Pichincha* . Obtenido de El skimming constituye una modalidad de fraude financiero dirigida específicamente contra tarjetas bancarias de débito y crédito. Esta técnica criminal opera mediante la extracción no autorizada de información almacenada en la banda magnética de las tarje

Salguero Diaz, D. (junio de 2017). *Grado en Seguridad y Control de Riesgos.* Obtenido de accedacris: https://accedacris.ulpgc.es/bitstream/10553/24768/4/0740277_00000_0000.pdf

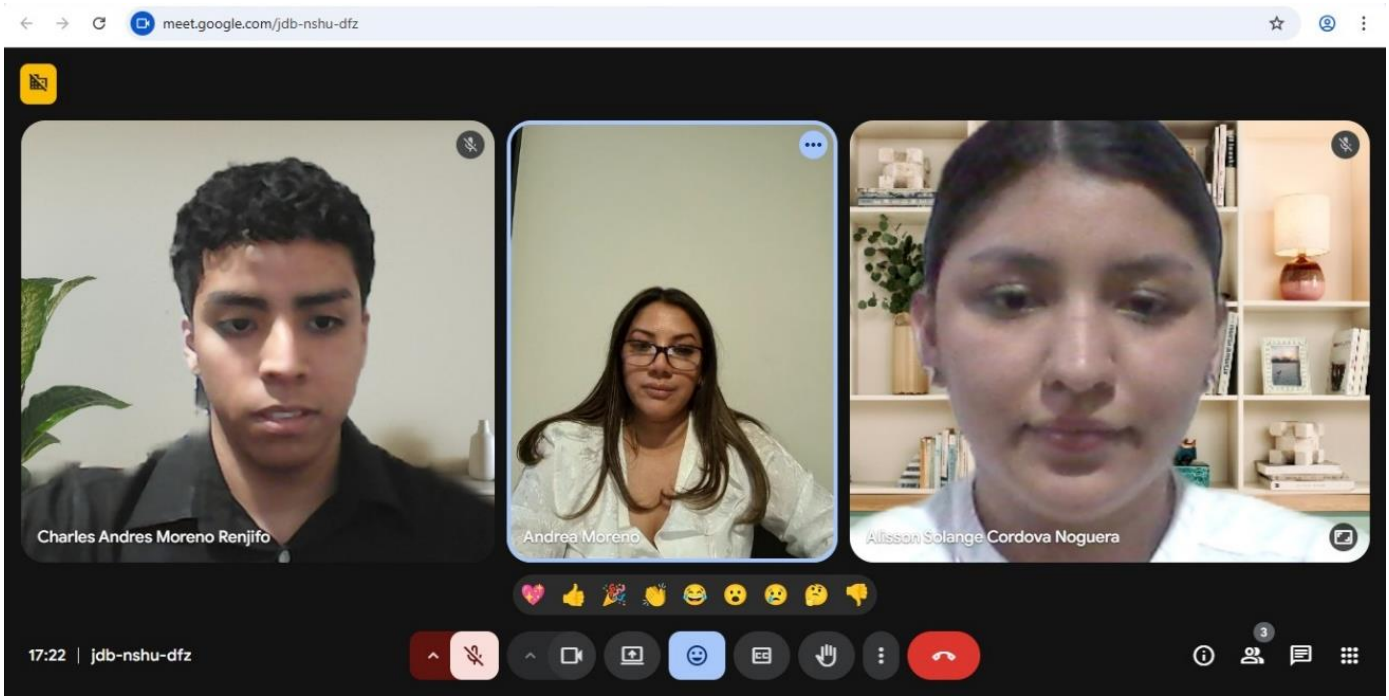
Zambrano, L. (5 de Mayo de 2025). Obtenido de https://www.expreso.ec/actualidad/economia/suplantacion-identidad-mal-aterra-multiplica-241350.html

ANEXOS

Anexo 1. Entrevista del Abogado Jaime Lenin Hurtado Angulo



Anexo 2. Entrevista de la Jueza Andrea Ivonne Moreno Silva



Anexo 3. Entrevista del Fiscal Marco Ordeñana Baldeón