**UNIVERSIDAD TECNOLOGICA ECOTEC**

**FACULTAD:**

**DERECHO Y GOBERNABILIDAD**

**TITULO:**

# “EL USO DE LA TECNOLOGIA EN LA COMISIÓN DE DELITOS FINANCIEROS Y SU IMPACTO EN LA SEGURIDAD JURÍDICA EN GUAYAQUIL”

**LINEA DE INVESTIGACIÓN:**

GESTION DE LAS RELACIONES JURIDICAS

**MODALIDAD DE TITULACION:**

VIRTUAL

**CARRERA:**

DERECHO

**TITULO A OBTENER:**

ABOGADO

**AUTOR:**

**Abdel Isaac Dahik Cabrera**

**TUTOR**

**Jaime Albán Mariscal**

**GUAYAQUIL 2023**

## DEDICATORIA

A mis padres, fuente inagotable de amor, sabiduría y apoyo incondicional. Su constante aliento y sacrificio han sido mi mayor inspiración a lo largo de este viaje académico.

A mis hermanos, cuya paciencia y comprensión han sido mi roca en los momentos desafiantes, brindándome la fortaleza necesaria para alcanzar cada meta.

A mis compañeros de carrera los cuales se convirtieron en mis amigos, por compartir risas, lágrimas y motivaciones a lo largo de esta travesía. Su amistad ha iluminado los días más oscuros y ha hecho que cada paso valga la pena.

A mis profesores y mentores, quienes han guiado mis pasos y compartido su conocimiento, dándome las herramientas necesarias para crecer como académico y como persona.

A todos aquellos que, de alguna manera, formaron parte de este viaje académico, gracias por ser parte fundamental de mi historia. Este logro no solo es mío, sino también de todos ustedes.

Finalmente, dedico este trabajo a mí mismo, como recordatorio de la perseverancia, el esfuerzo y la pasión que me llevaron hasta aquí. Que esta tesis sea un testimonio de mi dedicación y un punto de partida para nuevos horizontes.

Con gratitud,

Abdel Isaac Dahik Cabrera

## AGRADECIMIENTO

Quisiera expresar mi profunda gratitud a todas las personas que contribuyeron de manera significativa a la realización de este trabajo. Este proyecto no habría sido posible sin el apoyo y la colaboración de muchos individuos excepcionales.

Agradezco sinceramente a mi tutor de tesis, El abogado Jaime Alban por su guía experta, paciencia y dedicación a lo largo de este proceso. Sus valiosos comentarios y perspicaces sugerencias han sido fundamentales para dar forma a este trabajo de investigación.

Mi agradecimiento se extiende al departamento de la Facultad de Derecho y Gobernabilidad por proporcionar el entorno propicio para llevar a cabo esta investigación. Los recursos y facilidades ofrecidos han sido invaluables en el desarrollo de este proyecto.

Agradezco a mis profesores y tutores, cuyos conocimientos y orientación han sido una fuente constante de inspiración. Sus enseñanzas han enriquecido mi comprensión del tema y han contribuido de manera significativa a mi crecimiento académico.

No puedo dejar de expresar mi reconocimiento a mis compañeros de clase y amigos que compartieron sus ideas, experiencias y aliento a lo largo de este viaje. Sus perspectivas únicas y su apoyo moral han sido una parte integral de mi experiencia académica.

A mi familia, agradezco su amor incondicional, comprensión y respaldo constante. Su apoyo emocional ha sido mi mayor motivación y me ha dado la fortaleza para superar los desafíos.

Finalmente, agradezco a todos aquellos que, de alguna manera, contribuyeron a este proyecto. Este logro es el resultado del esfuerzo colectivo de muchos, y estoy agradecido por cada aportación.

Con aprecio,

Abdel Isaac Dahik Cabrera

## CERTIFICADO DE REVISION FINAL

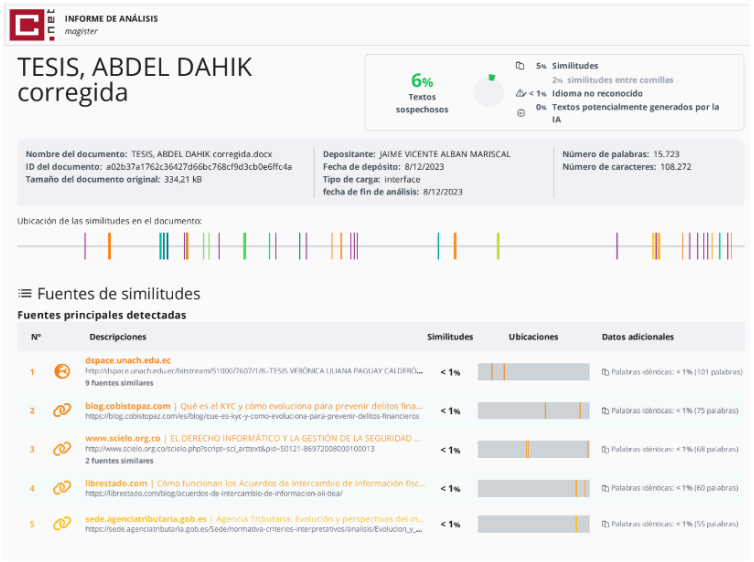
## ANEXO N°15

### CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

---

Habiendo sido nombrado Jaime Vicente Alban Mariscal tutor del trabajo de titulación “El uso de la tecnología en la comisión de delitos financieros y su impacto en la seguridad jurídica en Guayaquil” elaborado por Abdel Isaac Dahik Cabrera, con mi respectiva supervisión como requerimiento parcial para la obtención del título de abogado.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias de 6% mismo que se puede verificar en el siguiente link: https://mail.google.com/mail/u/0/#inbox/KtbxLthRWGjXSfXfCjJkLMlDQSdTtvMsnV?projector=1&messagePartId=0.1


INFORME DE ANÁLISIS
magister

TESIS, ABDEL DAHIK corregida

6% Textos sospechosos

5% Similitudes
2% similitudes entre comillas
< 1% Idioma no reconocido
0% Textos potencialmente generados por la IA

Nombre del documento: TESIS, ABDEL DAHIK corregida.docx
ID del documento: a02b37a1762c36427d66bc768cf9d3cb0e6ffc4a
Tamaño del documento original: 334,21 kB

Depositante: JAIME VICENTE ALBAN MARISCAL
Fecha de depósito: 8/12/2023
Tipo de carga: interface
fecha de fin de análisis: 8/12/2023

Número de palabras: 15.723
Número de caracteres: 108.272

Ubicación de las similitudes en el documento:

Fuentes de similitudes

Fuentes principales detectadas

| Nº | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | dspace.unach.edu.ec<br>http://dspace.unach.edu.ec/bitstream/51000/7607/1/8.-TESIS VERÓNICA LILIANA PAGUAY CALDERÓ...<br>9 fuentes similares | < 1% | | Palabras idénticas: < 1% (101 palabras) |
| 2 | blog.cobistopaz.com \| Qué es el KYC y cómo evoluciona para prevenir delitos fina...<br>https://blog.cobistopaz.com/es/blog/que-es-kyc-y-como-evoluciona-para-prevenir-delitos-financieros | < 1% | | Palabras idénticas: < 1% (75 palabras) |
| 3 | www.scielo.org.co \| EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD ...<br>http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013<br>2 fuentes similares | < 1% | | Palabras idénticas: < 1% (68 palabras) |
| 4 | librestado.com \| Cómo funcionan los Acuerdos de Intercambio de Información fisc...<br>https://librestado.com/blog/acuerdos-de-intercambio-de-informacion-all-clear/ | < 1% | | Palabras idénticas: < 1% (60 palabras) |
| 5 | sede.agenciatributaria.gob.es \| Agencia Tributaria: Evolución y perspectivas del in...<br>https://sede.agenciatributaria.gob.es/Sede/normativa-criterios-interpretativos/analisis/Evolucion_y_... | < 1% | | Palabras idénticas: < 1% (55 palabras) |

**FIRMA DEL TUTOR**

**Jaime Vicente Alban Marisca**

# ANEXO N°16

**CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL**

Samborondón 8 de agosto del 2023

Magíster

**Andrés Madero Poveda**

**Decano de la Facultad**

**Derecho y Gobernabilidad.**

Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: “El uso de la tecnología en la comisión de delitos financieros y su impacto en la seguridad jurídica en Guayaquil” según su modalidad PROYECTO DE INVESTIGACIÓN: REALIZADA DE MANERA **VIRTUAL**; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **Dahik Cabrera Abdel Isaac,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

**ATENTAMENTE,**

**Mgtr. Jaime Vicente Alban Mariscal**

**Tutor**

## RESUMEN

Esta investigación aborda el tema del cometimiento de delitos financieros haciendo uso de la tecnología y como se ven afectadas las personas de Guayaquil, el cual se centra en determinar cómo influye la regulación de los delitos financieros por medios digitales a la economía de Guayaquil y a la seguridad jurídica. El objetivo es proponer medidas efectivas para fortalecer la protección y prevención de estos delitos. La pregunta guía de esta investigación fue: ¿Cómo influye la regulación de los delitos financieros por medios digitales a la economía de Guayaquil y a la seguridad jurídica? Para el enfoque de investigación se usó el cuantitativo, de tipo no experimental transversal en la recolección de datos por medio de una encuesta. Los resultados de la encuesta indican una alta conciencia y preocupación entre los encuestados sobre los riesgos de seguridad en línea, especialmente en relación con las transacciones financieras. También existe una percepción generalizada de que las medidas legales y de seguridad actuales, pueden no ser suficientes para combatir eficazmente los delitos financieros en línea. Además, se delimitaron los delitos financieros digitales más comunes en la economía digital de Guayaquil. Para Finalizar, se puntualizó medidas efectivas para fortalecer la protección y prevención de los delitos financieros más comunes en la economía digital de Guayaquil.



**Palabras clave:** delitos financieros, economía digital, responsabilidad corporativa, información del cliente, sofisticación de delitos financieros, riesgos de seguridad en línea

## ABSTRACT

This research addresses the issue of committing financial crimes using technology and how people in Guayaquil are affected. It focuses on determining how the regulation of digital financial crimes influences the economy of Guayaquil and legal security. The objective is to propose effective measures to strengthen the protection and prevention of these crimes. The guiding question for this research was: How does the regulation of digital financial crimes influence the economy of Guayaquil and legal security? A quantitative, non-experimental cross-sectional approach was used for data collection through a survey.

Survey results indicate a high awareness and concern among respondents about online security risks, especially in relation to financial transactions. There is also a widespread perception that current legal and security measures may not be sufficient to effectively combat online financial crimes. Additionally, the most common digital financial crimes in the digital economy of Guayaquil were identified. In conclusion, effective measures were outlined to strengthen the protection and prevention of the most common financial crimes in the digital economy of Guayaquil.



Keywords: financial crimes, digital economy, corporate responsibility, customer information, sophistication of financial crimes, online security risks.

## Contenido

## INTRODUCCIÓN

En la era de la transformación digital y la economía globalizada, el uso generalizado de la tecnología ha traído consigo una serie de desafíos en el ámbito del derecho penal. En particular, la creciente incorporación de herramientas digitales en las transacciones financieras ha dado lugar a un preocupante aumento de los delitos financieros en Guayaquil. La sofisticación de los métodos utilizados por los delincuentes cibernéticos ha puesto en riesgo la seguridad jurídica y la estabilidad económica de la sociedad.

La presente investigación se centra en analizar la problemática del uso de la tecnología en la comisión de delitos financieros y su impacto en la seguridad jurídica en Guayaquil. En un entorno donde las relaciones económicas se han trasladado a plataformas digitales y las transacciones se realizan a través de medios electrónicos, resulta imprescindible comprender los retos que ello plantea en términos de regulación y aplicación de la ley.

El objetivo de este estudio es examinar cómo los avances tecnológicos han permitido la perpetración de delitos financieros, como el fraude electrónico, el robo de identidad y el lavado de dinero, y cómo estas actividades ilícitas afectan la estabilidad económica y la confianza en el sistema financiero de Guayaquil. Además, se buscó evaluar la eficacia de las leyes y medidas de seguridad actuales, así como proponer posibles soluciones para fortalecer la lucha contra los delitos financieros en el entorno digital.

En palabras de John F. Kennedy, expresidente de Estados Unidos (citado por Cesar Juárez, 2020), "el cambio es la ley de la vida. Y aquellos que solo miran al pasado o al presente seguramente perderán el futuro". Esta cita resalta la importancia de encontrar un equilibrio entre el avance tecnológico y la seguridad jurídica en el ámbito financiero. Con base en esta premisa, esta investigación se propone analizar y proponer soluciones efectivas que permitan salvaguardar los

intereses de la sociedad guayaquileña y mantener la integridad del sistema financiero en la era digital.

La ciudad de Guayaquil es un punto de referencia significativo en el Ecuador como lo es Cuenca o Quito, pero fue la ciudad escogida para esta investigación por el alto porcentaje de delincuencia en esta ciudad costeña, lo cual perjudica la seguridad jurídica.

**Conveniencia**

La importancia de esta investigación cunde dentro de un marco de resolución de un gran problema social que nos afecta en la actualidad en el Ecuador, el cual es los delitos cibernéticos y esta investigación servirá para mejorar la defensa de las personas en contra de los ciberdelincuentes y prevenir estafas a futuro, creando conciencia en las personas desconocedoras de los delitos cibernéticos e implementar nuevos desarrollos de leyes a la medida para crear un Ecuador más seguros.

**Relevancia**

Un futuro con un mayor conocimiento en la seguridad en el uso adecuando de las herramientas que nos aportan la tecnología informática y sentirnos más seguros en estas redes de información. Se creará nuevas herramientas de conciencia y leyes que beneficiaran la defensa de las personas que no conozcan los riegos de utilizar de manera incorrecta las redes de información de las webs y evitar ser estafadas de manera económica o por robo de identidad, dando a conocer las formas en las cuales los ciberdelincuentes cometen estas estafas y creando conciencia

El alcance que se intenta llevar a cabo con esta tesis es el de llegar de manera nacional a todo el público. Como implicaciones practicas se encuentra el hecho de que servirá a resolver los problemas de estafa digital

El problema que se busca resolver es el de los ciberdelitos en el ecuador, más centrado en los ciberdelitos que se llevan a cabo en guayaquil, los cuales desde

pandemia se han visto incrementados ya que, con las personas en pandemia, la delincuencia también fue desarrollando nuevas maneras llevar a cabo sus estafas

## PLANTEAMIENTO DE PROBLEMA

El problema que se pretende abordar en esta investigación es la falta de regulación efectiva de los delitos financieros cometidos a través de la tecnología en Guayaquil y su impacto negativo en la seguridad jurídica y la estabilidad económica. En la economía digital actual, se ha observado un aumento significativo de delitos como el fraude electrónico, el robo de identidad y el lavado de dinero, los cuales representan una amenaza para el correcto funcionamiento del sistema financiero y la confianza de los ciudadanos en las transacciones digitales.

La implementación generalizada de sistemas de pago electrónicos, como tarjetas de crédito, débito y otros métodos, ha simplificado las operaciones financieras, pero también ha dado lugar a nuevas formas de delitos financieros, como la estafa, tal como se describe en el artículo 186 del COIP (Asambrea Nacional, 2021)

Los avances en la clonación de tarjetas, el uso de dispositivos electrónicos para la obtención fraudulenta de información financiera y otras tácticas engañosas han llevado a un aumento en los casos de estafas financieras. Por tales motivos, es necesario identificar las nuevas formas de delitos que se cometen a través del internet, en especial cuando se efectúan las compraventas entre las personas 3 con el ánimo de causar daño. Por ello se deberían proponer algunas alternativas de solución a esta problemática de índole económico, social y tecnológico. (CALDERÓN, 2020, págs. 2-3)

La regulación efectiva de los delitos financieros en la economía digital es esencial para preservar la confianza en el sistema financiero y garantizar la seguridad jurídica en las transacciones digitales. La falta de normas específicas y

la adaptación lenta de la legislación a los avances tecnológicos representan un desafío en la lucha contra el fraude electrónico, el robo de identidad y el lavado de dinero en el contexto digital.

Hasta ahora, se ha realizado cierto progreso en la regulación de los delitos financieros tradicionales, pero existe una brecha significativa en cuanto a la adaptación de la legislación penal a los nuevos desafíos planteados por la tecnología. La falta de normas específicas y la complejidad de la investigación y persecución de los delitos cibernéticos han dificultado la protección de los derechos de las víctimas y la imposición de sanciones adecuadas a los perpetradores.

Los resultados esperados de esta investigación son, en primer lugar, identificar las deficiencias en la legislación actual relacionada con los delitos financieros en el ámbito digital. Además, se busca proponer recomendaciones y estrategias para fortalecer la regulación y aplicación de la ley, con el fin de garantizar la seguridad jurídica y la estabilidad económica en Guayaquil. Asimismo, se espera generar conciencia sobre la importancia de abordar esta problemática y promover el trabajo conjunto entre las autoridades, las instituciones financieras y la sociedad en general.

Para llevar a cabo esta investigación, se utilizó un enfoque metodológico cuantitativo que incluirá revisión bibliográfica, análisis de legislación vigente, encuesta sobre la confianza en la regulación de los delitos financieros en la economía digital de guayaquil. Se buscó obtener datos relevantes y análisis sólidos que respalden las conclusiones y recomendaciones planteadas en este estudio.

A continuación, se plantea la pregunta problémica: ¿Cómo influye la regulación de los delitos financieros por medios digitales a la economía de Guayaquil y a la seguridad jurídica?

## HIPOTESIS

La falta de regulación de los delitos financieros por medios digitales afecta a la economía de Guayaquil y la seguridad jurídica.

## OBJETIVOS DE INVESTIGACION

### 1. OBJETIVO GENERAL

Determinar cómo influye la regulación de los delitos financieros por medios digitales a la economía de Guayaquil y a la seguridad jurídica

### 2. OBJETIVOS ESPECIFICOS

2.1 Diagnosticar el impacto en la seguridad jurídica sobre la regulación de los delitos financieros en la economía digital de Guayaquil.

2.2 Determinar los delitos financieros más comunes en la economía digital de Guayaquil

Proponer medidas efectivas para fortalecer la protección y prevención de los delitos financieros más comunes en la economía digital de Guayaquil

## JUSTIFICACION

La creciente utilización de la tecnología en la comisión de delitos financieros plantea un desafío significativo para la seguridad jurídica en Guayaquil. Con el advenimiento de nuevas tecnologías y la expansión de la infraestructura digital,

los delincuentes han encontrado nuevas formas de cometer delitos financieros de manera más sofisticada, desafiando la efectividad de los sistemas de seguridad existentes.

Es importante entender que cada año es más normal los delitos electrónicos como las estafas y falsificaciones de identidad como lo refleja el estudio mostrado por Infobae (Blanco , 2022) el cual dice que alrededor del 2021 se registró un aumento interanual de incidentes informáticos del 261% como modificaciones de información virtual y spam.

Según la policía nacional del ecuador los delitos más frecuentes son la estafa por medios electrónicos los cuales son estafas de Phishing, estafa de Spear Phishing y estafas de Smishing (Toala Indio, 2021)

El objetivo principal de esta tesis es analizar y comprender el impacto de la tecnología en la comisión de delitos financieros y evaluar sus implicaciones en la seguridad jurídica en Guayaquil. A través de una investigación exhaustiva, se buscará identificar las tendencias emergentes en el uso de la tecnología para cometer delitos financieros y examinar cómo dichos delitos afectan la confianza en el sistema jurídico y financiero de la ciudad.

El artículo 186 (Asambrea Nacional, 2021) del Código Orgánico Integral Penal de Ecuador establece un marco legal sólido para sancionar las diversas formas de estafa perpetradas mediante la manipulación tecnológica, lo que resalta la urgente necesidad de una investigación en profundidad sobre este fenómeno. La creciente sofisticación de las técnicas delictivas respaldadas por la tecnología ha llevado a una serie de consecuencias nefastas para la seguridad jurídica en Guayaquil, afectando la confianza en las transacciones financieras y minando la integridad del sistema financiero. La investigación de este tema permitirá identificar y comprender las tendencias emergentes en la utilización de la tecnología para la comisión de delitos financieros, evaluar la efectividad de las regulaciones actuales

contempladas en el artículo 186 y proponer medidas concretas para fortalecer la seguridad jurídica y proteger los intereses económicos de los ciudadanos y el tejido empresarial en Guayaquil.

Esta investigación es de vital importancia, ya que permitirá a las autoridades guayaquileñas comprender las nuevas formas de delincuencia financiera impulsadas por la tecnología y tomar medidas para prevenirlas y combatirlas de manera más efectiva. Además, proporcionará una base sólida para el desarrollo de políticas y regulaciones actualizadas que se adapten a los avances tecnológicos y protejan la seguridad jurídica en el entorno financiero.

Asimismo, esta tesis busca promover la concienciación y educación sobre los riesgos asociados con la tecnología y los delitos financieros entre las instituciones financieras, los profesionales del derecho y los ciudadanos en general. La información y las recomendaciones resultantes de este estudio podrán utilizarse para fortalecer las capacidades de ciberseguridad, mejorar los mecanismos de detección y prevención de delitos financieros y fomentar una mayor colaboración entre las instituciones involucradas en la seguridad jurídica en Guayaquil.

**Relevancia Social.** - Guayaquil es una ciudad está creciendo constantemente y es una de las ciudades más importantes del ecuador tanto social como económico por lo cual la problemática planteada puede aumentar con el paso del tiempo

**Implicaciones jurídicas. –** Desde una perspectiva jurídica se debe analizar las reformas y demás implementaciones que se pueden llegar a desarrollar para regular la manera de disminuir el cometimiento de delitos sobre la economía digital

# CAPITULO I
# REVISION LITERATURA

## 1.Definiciones conceptuales

### 1.1 Delitos financieros

Delito es todo acto que atente contra un tercero ya sea física, moral, o psicológica, en este caso el delito financiero hace alusión a que el patrimonio monetario de una persona se ve afectado por el causante del acto, ya sea un robo, fraude por personas mal intencionadas u operaciones transaccionales por medio de engaños de grupos delictivos afectan un patrimonio financiero por lo cual engloba el concepto de un delito financiero.

Para sintetizar de mejor manera el concepto delito financieros, la interpol en un artículo de su página principal menciona que “se trata de actividades delictivas graves cuya importancia no debería minimizarse pues, más allá del impacto social y económico, por lo general están estrechamente vinculadas con la delincuencia violenta e incluso el terrorismo” (Interpol, 2023).

### 1.2 Tecnología

La definición de tecnología provine de la unión de dos palabras, técnica y ciencia. La técnica es el grupo de procesos que se tienen aprendidas para desarrollar e implementar algún tipo de actividad de forma más controlada y corriendo menos riesgo de fallo.

Por otro lado; se denomina ciencia a todo el conocimiento o saber constituido mediante la observación y el estudio sistemático y razonado de la naturaleza, la sociedad y el pensamiento (Fernandez, 2022).

La tecnología es un conjunto de conocimientos sobre técnicas que al pasar los años se fueron puliendo para llegar a donde estamos actualmente, con el avance de tecnológico es decir el desarrollo de instrumentos que van evolucionando constantemente para llevar a cabo actividades de manera más simples con el uso de técnicas. Es un concepto amplio que abarca una gran variedad de aspectos y disciplinas dentro de la electrónica, el arte o la medicina (Editorial etece, 2022).

### 1.3 Uso de la tecnología

El uso de la tecnología en este caso el uso de tecnología enfocada en lo electrónico que es lo más habitual y muchas veces obligatoria para todo tipo de personas en la actualidad por el ecosistema informático que manejamos actualmente, la velocidad de los trabajos, los estudios y captación de información y envió de información si usamos la tecnología como celulares , laptops o tables para el día a día estaríamos desacoplados del ecosistema actual y nos dejaría muy atrás en comparación de las demás personas.

Hace 10 años era frecuente ver a personas de edad más avanzada desconocer el uso de la tecnología como el celular, pero en la actualidad esto es cada vez más frecuente por la implementación de aplicaciones que generan endorfinas de satisfacción en el momento de óseo como lo hacen aplicaciones como Instagram o la que es tendencia actualmente la aplicación china llamada TikTok.

Estas aplicaciones son de acceso gratuito y sumamente intuitivas en el caso de TikTok ni si quiera es necesario crearse una cuenta para poder empezar a usarla y pasar horas de horas frente a la pantalla del celular con entretenimiento

básico, pero tan corto que hace que generes la cantidad necesaria de endorfinas como para no despegarte del móvil y que el tiempo se vaya volando.

### 1.4 Desinformación

Pese a que el uso de aplicaciones gratuitas como las redes sociales parecieran ser del todo inofensivas, la realidad, es que se maneja una cantidad de información masiva y tan rápida creando una confianza con el consumidor la cual nunca se pone en tutela de juicio y ahí es cuando genera el verdadero problema.

Como ejemplo tenemos muchos casos en las cuales información ficticia de alguna red social se haya hecho viral, como el afamado caso de supuestas filtraciones sobre documentación y fotos de personas importantes de la presidencia de estados unidos los cuales eran acusados de ser reptilianos lo cual es algún tipo de raza alienígena inventado por los internautas.

Otros mitos de internet bastante conocidos son los casos de famosos fallecidos como lo son Michael Jackson o juan Gabriel los cuales aún existen muchos rumores de que nunca murieron o que buscaron una vida alejada de la fama y por eso fingieron su muerte.

### 1.5 Estafa

La palabra estafa tiene un gran peso según la RAE (Real Academia Española) estafa es un “delito que consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro” (Real Academia Española, 2001); dando un análisis corto, pero claro sobre la definición según el diccionario del español.

En el Ecuador el delito de estafa está estipulado en el artículo 186 del Código Integral Penal del Ecuador en el cual “la persona que, para obtener un beneficio

patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera" (La Asamblea Nacional , 2014).

## 2. Uso de la tecnología para el cometimiento de delitos financieros

El uso de la tecnología en el ámbito financiero ha dado lugar a una nueva dimensión de riesgos y desafíos, en la cual los delincuentes aprovechan avanzadas herramientas tecnológicas para perpetrar delitos financieros de manera más sofisticada y encubierta. La digitalización de las transacciones financieras ha brindado a los actores malintencionados una gama de oportunidades para llevar a cabo actividades ilícitas, incluyendo el robo de identidad, fraudes electrónicos y la manipulación de sistemas financieros. La criptomoneda, por ejemplo, ha emergido como una herramienta atractiva para los delincuentes debido a su naturaleza descentralizada y pseudónima, dificultando la trazabilidad de las transacciones ilícitas.

La rapidez con la que evolucionan las tecnologías financieras y la falta de una regulación adecuada han exacerbado aún más los riesgos asociados con el uso de la tecnología para cometer delitos financieros. La inteligencia artificial y el aprendizaje automático, por ejemplo, pueden ser empleados para eludir sistemas de seguridad tradicionales, adaptándose de manera dinámica a medidas de defensa. Este escenario plantea la necesidad crítica de comprender y abordar las complejidades que rodean la intersección entre la tecnología y los delitos financieros, con el fin de desarrollar estrategias eficaces de prevención y regulación.

## 3. Seguridad jurídica en el contexto financiero

La "seguridad jurídica" en el ámbito financiero se refiere a la certeza y confiabilidad proporcionadas por el marco legal y regulatorio que rige las transacciones financieras. Este concepto es esencial para garantizar la estabilidad, transparencia y protección de los derechos de todas las partes involucradas en operaciones financieras.

## 4. En el contexto financiero, la seguridad jurídica implica:

### 4.1- Claridad Normativa

La existencia de leyes y regulaciones específicas que definen claramente los derechos y responsabilidades de las instituciones financieras, los inversores y otros actores relevantes. Estas normativas deben ser comprensibles y de fácil acceso para todas las partes interesadas.

La claridad normativa requiere una tipificación unívoca de los supuestos de hecho que evite, en los posible, el abuso de conceptos vagos e indeterminados, así como una delimitación precisa de las consecuencias jurídicas. (Enrique, 2000)

### 4.2-Protección de Derechos

Asegurar que los derechos legales y contractuales de los individuos y entidades involucradas en transacciones financieras estén protegidos. Esto incluye garantizar la ejecución y cumplimiento de contratos, así como la protección de la propiedad y otros derechos fundamentales.

### 4.3-Previsibilidad

La capacidad de prever y anticipar las consecuencias legales de las acciones en el ámbito financiero. La estabilidad en las leyes y su aplicación

contribuye a la previsibilidad, permitiendo a las partes tomar decisiones informadas y gestionar riesgos de manera efectiva.

“La certeza del Derecho supone la faceta subjetiva de la seguridad jurídica, se presenta como la proyección en las situaciones personales de la seguridad objetiva” (Enrique, 2000).

### 4.4- Imparcialidad y Justicia

Garantizar que las decisiones legales relacionadas con asuntos financieros se tomen de manera imparcial y justa, sin discriminación ni favoritismo hacia ninguna parte. La aplicación equitativa de la ley es esencial para mantener la confianza en el sistema financiero.

se centran en garantizar un tratamiento equitativo para todas las partes involucradas, independientemente de su estatus social, económico o cualquier otra característica distintiva. Este principio fundamental implica que las leyes y su aplicación deben ser imparciales, sin favorecer a ninguna parte y sin discriminación. En otras palabras, la justicia legal se esfuerza por ofrecer un terreno de juego nivelado para todos los ciudadanos, instituciones y entidades que participan en el ámbito legal.

Para lograr la imparcialidad y justicia en el sistema legal, es crucial que las leyes sean formuladas y aplicadas de manera objetiva. Esto implica que los procedimientos judiciales deben basarse en hechos y pruebas, y las decisiones deben tomarse sin prejuicios ni influencias indebidas. Además, la transparencia en la interpretación y aplicación de las leyes es esencial para mantener la confianza del público en el sistema judicial. En última instancia, la imparcialidad y justicia no solo son principios fundamentales para el funcionamiento efectivo del sistema legal, sino que también son

pilares clave para la preservación de la seguridad jurídica en cualquier sociedad.

### 4.5- Aplicación Efectiva

La existencia de un sistema legal que no solo establece normas, sino que también garantiza su aplicación efectiva. Esto implica la existencia de mecanismos judiciales y administrativos eficientes para resolver disputas y hacer cumplir las leyes financieras.

En el marco de la tecnología y los delitos financieros, la seguridad jurídica se ve desafiada por nuevas formas de transacciones, como las criptomonedas, y la necesidad de adaptar el marco legal a la evolución tecnológica. La seguridad jurídica efectiva en el ámbito financiero no solo protege a los individuos y las instituciones, sino que también contribuye a la integridad y estabilidad del sistema financiero en su conjunto.

## 5. FRAUDE FINANCIERO

El fraude financiero es una práctica engañosa que busca obtener beneficios económicos de manera ilícita a expensas de individuos, empresas o instituciones financieras tal actividad delictiva abarca diversas formas, desde la falsificación de documentos hasta la manipulación de información con el propósito de inducir a error a inversores o entidades financieras. Un ejemplo común de fraude financiero es el fraude hipotecario, donde se utilizan prácticas engañosas para obtener préstamos hipotecarios bajo condiciones falsas o poco claras, perjudicando tanto a prestamistas como a prestatarios.

La complejidad del fraude financiero ha evolucionado con la tecnología, dando lugar a delitos como el phishing y el robo de identidad en línea. Estas actividades ilegales suelen involucrar la manipulación de información sensible, como números de tarjetas de crédito o contraseñas, para acceder a cuentas financieras y realizar transacciones fraudulentas. La prevención y detección efectiva del fraude financiero requieren una combinación de medidas legales, tecnológicas y de educación pública para mitigar el impacto negativo en la seguridad y confianza en los sistemas financieros.

Según una investigación que se realizó en España en el año 2020, redacta que el fraude financiero se visibiliza más durante la crisis económica, así como la necesidad de su resolución administrativa y jurídica (Rodriguez, Daniel, & Ana, 2020), esta frase señala una conexión entre el fraude financiero y las crisis económicas, destacando cómo este fenómeno se vuelve más evidente y problemático en momentos de crisis. Durante periodos económicos difíciles, es posible que las presiones financieras y la incertidumbre impulsen a algunos individuos o entidades a participar en prácticas fraudulentas para asegurar beneficios ilícitos o para evitar pérdidas. Esta dinámica puede agravar los desafíos económicos existentes y socavar la confianza en los sistemas financieros.

Además, la frase sugiere que abordar el fraude financiero durante una crisis económica requiere tanto medidas administrativas como jurídicas. La resolución administrativa podría referirse a acciones internas dentro de las instituciones financieras, como la implementación de controles más estrictos, auditorías y políticas de cumplimiento. Por otro lado, la resolución jurídica destaca la importancia de la aplicación de leyes y regulaciones específicas, así como la persecución de aquellos que participan en actividades fraudulentas. La combinación de ambas dimensiones es esencial para abordar de manera integral y efectiva los desafíos que

plantea el fraude financiero durante crisis económicas, contribuyendo así a la restauración de la confianza y la estabilidad en el sistema financiero.

## 6. Fraude Informático

Para (Altamirando, 2020) “la noción de fraude informático se vincula con la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos”. También (Altamirando, 2020) hacen hincapié que, “en segundo lugar, el concepto de fraude informático en ocasiones es relacionado con comportamientos que corresponden a otros delitos informáticos o a otros ciber-delitos.”

En su artículo Laura & Guillermo (2020), dejan claro que el fraude informático emerge como un protagonista indiscutido, siendo central en el escenario delictivo contemporáneo. Su importancia práctica se manifiesta en el impacto económico significativo que provoca y en su ejecución frecuente, particularmente en el contexto del auge del comercio electrónico. Este fenómeno delictivo, en constante evolución desde hace tres décadas, ha captado la atención de la doctrina penal, generando la necesidad de un estudio sistemático para comprender su naturaleza y delimitar sus fronteras legales.

A pesar de la atención que ha recibido, persiste la falta de claridad en torno a la definición precisa de fraude informático. El término abarca una variedad de conductas, desde la manipulación de datos hasta prácticas como el phishing y el pharming. La delimitación de este delito se ve desafiada por la inclusión de conductas relacionadas y su conexión con otros delitos informáticos, como el hacking. La necesidad de una comprensión clara y precisa de lo que implica llevar a cabo un comportamiento constitutivo de fraude informático se vuelve evidente en este contexto de constante cambio y complejidad en la ciber-criminalidad.

La vinculación a fraude informático con la palabra hacking es algo muy común dado que muchas personas lo usan como sinónimos de ciberdelitos muchas veces lo cual es erróneo. El término "hacking" se utiliza para describir la acción de explorar y manipular sistemas informáticos, a menudo con habilidades técnicas avanzadas, con el fin de comprender, modificar o acceder a información que no debería ser accesible. Si bien no todos los actos de hacking son maliciosos, aquellos realizados con intenciones dañinas se consideran delitos cibernéticos.

Por otro lado, El concepto de "ciberdelitos" abarca un conjunto amplio de actividades delictivas que involucran el uso de tecnología y redes informáticas. Esto incluye no solo el hacking, sino también actividades como el robo de datos, el fraude en línea, la distribución de malware, el phishing y otras acciones delictivas que aprovechan la tecnología como medio para cometer actos ilegales. Los ciberdelitos pueden variar en forma y afectar tanto a individuos como a organizaciones.

El fraude informático es una modalidad delictiva que se vale de la tecnología y los sistemas informáticos para realizar actividades fraudulentas. Este tipo de fraude abarca una variedad de prácticas, desde el phishing hasta la infiltración de sistemas mediante software malicioso. Los estafadores buscan explotar vulnerabilidades en la seguridad cibernética con el fin de obtener información confidencial, como contraseñas, datos financieros o de identificación personal. Además, el fraude informático puede manifestarse a través de esquemas más sofisticados, como la manipulación de sistemas electrónicos de pago o el ransomware, donde los delincuentes cifran datos y exigen un rescate para su liberación. Este tipo de delito no solo plantea riesgos significativos para la seguridad y privacidad de los individuos y las empresas, sino que también destaca la necesidad de constantes actualizaciones en las medidas de seguridad digital y la concienciación pública para prevenir y combatir eficazmente estas amenazas.

## 7. Antecedentes Históricos Y Contexto Internacional

Según Palma D. (2020), en su artículo “La delincuencia Económica en Chile: antecedentes teóricos e históricos sobre los “ladrones de levita y guante”, 1880-1920” el afirma que en las décadas finales del siglo XIX y las primeras del siglo XX en Chile, se gestaron delitos económicos que han desempeñado un papel fundamental en el proceso de configuración y perpetuación del orden social y económico capitalista que perdura hasta la actualidad. Estos actos delictivos, en su diversidad y complejidad, no solo marcaron el devenir histórico de la nación, sino que también contribuyeron a cimentar las bases sobre las cuales se ha edificado la estructura económica y social chilena contemporánea. El análisis de estos delitos económicos no solo revela su impacto inmediato en el tejido social de la época, sino que arroja luz sobre la continuidad de sus repercusiones en la conformación de la realidad económica y social del país en el transcurso de los años.

Para Baracaldo Lozano & Daza Giraldo, (2015) en su investigacion “Panorama de los currículos de programas de contaduría pública en Colombia frente a contenidos de auditoría forense y prevención de delitos financieros” explican que la creciente incidencia de delitos económicos y financieros, como fraude financiero, corrupción y prácticas empresariales cuestionables, tanto a nivel local como internacional, subraya la imperiosa demanda de contar con expertos capacitados en la investigación y análisis de estas conductas. La auditoría forense emerge como una herramienta esencial para abordar este desafío, desempeñando un papel crucial en la detección, documentación y comprensión de los intricados entramados que caracterizan estos delitos. La necesidad de profesionales altamente especializados en este campo se torna evidente, ya que la complejidad y sofisticación de estos actos delictivos exigen un enfoque diligente y experto para salvaguardar la integridad del entorno empresarial y financiero. En este contexto, la auditoría forense se erige como un componente esencial en la respuesta a la creciente complejidad de los delitos financieros, proporcionando las habilidades necesarias para enfrentar eficazmente estos desafíos contemporáneos.

La Representante en  Chile y coordinadora de Capacitaciones a nivel mundial Lopez Garcia, (2021) en su investigacion “Evolucion De Las Finanzas Sostenibles En America Latina Y El Caribe” detalla que en términos generales, América Latina y el Caribe han presenciado notables progresos en el ámbito de las finanzas sostenibles, marcados por la introducción de regulaciones y políticas destinadas a prevenir y castigar los delitos financieros. A pesar de estos avances, persisten desafíos significativos en cuanto a la aplicación efectiva de estas medidas. La región se encuentra en un proceso dinámico de fortalecimiento de sus marcos regulatorios para hacer frente a las complejidades de los delitos financieros, abordando áreas clave como el lavado de dinero, la corrupción y otras prácticas ilícitas. No obstante, la eficacia plena de estas iniciativas se ve obstaculizada por obstáculos que van desde limitaciones en la capacidad institucional hasta la necesidad de mejorar la coordinación interinstitucional y la cooperación internacional. Así, a pesar de los logros alcanzados, se reconoce la existencia de retos pendientes que requieren una atención continua para garantizar una implementación eficiente y completa de las políticas diseñadas para combatir los delitos financieros en la región.

En palabras de los investigadores, Rubio Rodriguez, Guido Hernandez, & Lopez Blandon, (2021) después de un análisis de las grandes y pequeñas empresas financieras llegaron a la conclusión que A pesar de la presunción general de que las herramientas informáticas son aliadas esenciales para el control organizacional en la era digital, se identifican niveles deficientes de apropiación tecnológica en el ámbito de control y aseguramiento del riesgo, según las entidades examinadas. Estos hallazgos evidencian brechas en la actualización tecnológica, en la dimensión de desarrollo organizacional de los directivos y en la construcción del ideario regional sobre los riesgos a los que se enfrentan las entidades que carecen de una infraestructura tecnológica sólida. Esta disparidad plantea desafíos significativos y destaca la importancia

de abordar las deficiencias tecnológicas para fortalecer la capacidad de control y gestión de riesgos en el entorno organizacional.

Para los investigadores Gómez, M.B., Díaz, H.M., & Quintero, P.S. (2020) en su investigación “Determinación de los ataques cibernéticos claves a través de la técnica MICMAC y su influencia económica financiera al adquirir herramientas de seguridad automatizada” detallan que, en el ámbito de la ciberseguridad, diversos métodos maliciosos son empleados por hackers para acceder a sistemas informáticos. Los ataques a correos electrónicos, conocidos como phishing, buscan engañar a usuarios para obtener información confidencial. Los virus informáticos son programas maliciosos que se propagan y pueden dañar o controlar sistemas. Los gusanos son similares, pero se replican automáticamente sin necesidad de intervención humana. Los hackers también aprovechan vulnerabilidades en software y sistemas operativos para infiltrarse. Estos métodos subrayan la importancia de medidas preventivas, como actualizaciones de seguridad y concienciación sobre prácticas seguras en línea.

Según la investigación de Chavez Bravo, Malpartida Marquez , Villacorta Cavero, & Orellano Antunez (2020), en su “investigacion La influencia de la automatización inteligente en la detección del cibercrimen financiero” afirmaron que los delitos cometidos en la pandemia reciente fueron de uso tecnológico por que la inmensa mayoría de  ataques contra empresas y usuarios se llevaron a cabo mediante actos delictivos de carácter financiero, y de los que fueron víctimas, utilizando ransomware, phishing y robo de criptomonedas.

El 25,10% de ataques de ransomware (secuestro de datos) en el 2017 fueron identificados en nuestro país, la cifra más alta en América Latina, según la empresa de seguridad Eset. Los ciberdelincuentes también aprovecharon vulnerabilidades, y en Perú, una de las amenazas de este tipo fue EternalBlue,

que utilizó para difundir WannaCry en 2017 y causó daños a, decenas de empresas peruanas y, más de 200.000 sistemas afectados en 150 países

También afirmaron Chavez Bravo, Malpartida Marquez , Villacorta Cavero, & Orellano Antunez (2020), que otro problema que dificulta la detección del ransomware es que el ataque no se lleva a cabo de forma inmediata. Según un estudio de EY Perú, el 47% de las empresas peruanas dijeron que era poco probable que detectaran un ciberataque sofisticado en el corto plazo.

El incidente más sonado en Perú fue el ciberataque a la naviera del grupo danés Maersk. Esta empresa fue víctima de la variante del ransomware Petya. En Perú se detectan dos tipos de malware “minero”, que buscan utilizar la potencia de procesamiento del dispositivo del usuario para obtener criptomonedas mediante cifrado y minería directamente desde la computadora, laptop u otro. A esto se suma otro código malicioso popular en Perú llamado HoudRat. EL RAT (Remote Access Tool) está destinada a controlar dispositivos informáticos para permitir el acceso remoto a los ciber atacantes.

En medio de la actual pandemia, Perú sufrió 613 millones de ciberataques de enero a junio de 2020. Mientras tanto, en América Latina y el Caribe, la cifra alcanzó los 15 mil millones, según el informe 2020Q2 Threat Intelligence Insider Latin America de la plataforma de inteligencia Fortinet, que recopila y analiza. Investigue incidentes de seguridad cibernética en todo el mundo. Sólo en el último trimestre, empresas experimentaron un aumento significativo en los ataques de "fuerza bruta", o intentos repetidos y sistemáticos de piratear algoritmos y adivinar credenciales mediante el envío de nombres de usuario y contraseñas de inicio de sesión diferentes a través de correo electrónico, redes sociales y Wi-Fi, entre otros. El crecimiento del trabajo y el aprendizaje remotos ha despertado el interés de los piratas informáticos por los ataques de “fuerza bruta”. Con el cambio masivo al aprendizaje en la oficina y en el hogar, los ciberdelincuentes se enfrentan a una cantidad significativa de servidores de

Protocolo de escritorio remoto (RDP) mal configurados, lo que hace posible que este tipo de ataques

Chavez Bravo, Malpartida Marquez , Villacorta Cavero, & Orellano Antunez (2020), demostraron en su investigacion que los delitos financieros por el uso de medios tecnologicos tenia un crecimiento ecponencial. Chavez Bravo, Malpartida Marquez , Villacorta Cavero, & Orellano Antunez, (2020) La búsqueda se orientó a la automatización inteligente asociada a la detección de los crímenes financieros, en las empresas de servicios financieros, empresas de comercio electrónico, organizaciones gubernamentales y bancos de los países de Estados Unidos y Perú principalmente. En total se encontraron 34.390 casos; de los cuales 14.429 casos corresponden a cyber attack y 20.000 casos a crime finance al gobierno de los Estados Unidos y empresas financieras respectivamente, 209 casos corresponden a cost of fraud en empresas minoristas, comercio electrónico, banca y finanzas respectivamente.

El Señor Velasco Melo en su trabajo “EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001” hace un análisis de el por qué el uso de la tecnología y como se engloba el mundo con el avance tecnológico y capitalista genera cambios en nuestra forma de vida por la cual nosotros debemos evolucionar y comparar las defensas que teníamos anteriormente con las nuevas amenazas que vienen, pese que esta investigación sea del 2007 La metodología utilizada para contabilizar los distintos impactos corresponde a la de la norma ISO 27001 en áreas relacionadas con el cumplimiento. Esto incluye:

Protección de Datos Personales. Celebración de contratos de productos informáticos y telemáticos. Leyes de trabajo y servidumbre en materia de regulación de aspectos técnicos. servicios de comercio electrónico, propiedad intelectual y gestión de incidentes informáticos. Haciendo una comparativa con

una amenaza actual y comparándola con la protección que nos da la norma ISO 27001 la cual contempla diez dominios:

1.-Política de Seguridad de la Información

2.-Organización de la Seguridad de la Información

3.-Gestión de Activos

4.-Seguridad de Recursos Humanos

5.-Seguridad Física y del Entorno

6.-Gestión de Comunicaciones y Operaciones

7.-Control de Acceso

8.-Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

9.-Gestión de Incidentes de la Seguridad de la Información

10.-Cumplimiento

Gracias a la comparativa podemos comprender los requisitos de seguridad de la información del negocio y la necesidad de establecer objeticos en relación con la seguridad de la información. Comprender que por lo globalizado que esta el mundo actualmente el dar nuestra información a grandes empresas no nos deja exentos de por ser estafados por personas que sean conocedoras de técnicas de hackeo sofisticadas y muchas veces pueden incluso afectar a empresas internacionales y puede caer nuestras cuentas bancarias en personas que no son deseadas.

Por eso es importante que las grandes empresas inviertan constantemente en nuevas implementaciones de protección y hagan un sondeo de las personas afectadas, haciendo una mejora continua basada en la medición de objetivos.

En un entorno donde la legislación aplicable en temas de tecnologías de la información y las comunicaciones es escasa, el contenido y desarrollo de las políticas que las organizaciones desarrollan en esta materia cobran mayor importancia. Además, la presencia de empresas de diferentes sectores económicos implica el cumplimiento de una amplia gama de normas legales, lo que dificulta la armonización de estos principios específicos con las nuevas tendencias del derecho.

Además, el informe sobre tecnología e información 2021 publicado en la Conferencia de las Naciones Unidas sobre comercio y desarrollo (UNCTAD) encamina como los países en desarrollo pueden subirse a la ola de la tecnología de frontera y compaginar innovación con equidad en sus intentos de lograr los objeticos de desarrollo sostenible que se llevan a cabo en cada país

## 8. TECNOLOGIAS UTILIZADAS EN DELITOS FINACIEROS

Las tecnologías utilizadas en delitos financieros son diversas y están en constante evolución. Algunas de las técnicas comunes asociadas con estos delitos incluyen:

### 8.1-Phishing

Se emplean correos electrónicos falsos o sitios web fraudulentos para engañar a las personas y obtener información confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito.

### 8.2- Malware y Spyware

Programas maliciosos infectan sistemas informáticos para recopilar información financiera, como keyloggers (registros de pulsaciones de teclas) o spyware (recolección de información sin conocimiento del usuario).

### 8.3- Ingeniería Social

Se utilizan tácticas de manipulación psicológica para engañar a las personas y obtener información confidencial, como haciéndose pasar por representantes de servicios financieros.

### 8.4- Ataques de Ransomware

Cifran archivos y exigen un rescate para restaurar el acceso, y los pagos suelen solicitarse en criptomonedas para dificultar el rastreo.

### 8.5- Tarjetas Clonadas y Skimming

Los delincuentes copian información de tarjetas de crédito mediante dispositivos de skimming en cajeros automáticos o lectores de tarjetas comprometidos.

### 8.6- Fraude en Transacciones Financieras en Línea

Se realizan transacciones fraudulentas en línea utilizando información robada o falsificada.

### 8.7- Criptomonedas

Con la popularidad creciente de las criptomonedas, también aumentan los delitos financieros relacionados, como estafas de inversión y hackeos de intercambios de criptomonedas.

### 8.8- Operaciones de Lavado de Dinero

Se emplean diversas tecnologías para ocultar la procedencia ilícita de fondos, como el uso de criptomonedas, transacciones en efectivo y estructuras empresariales complejas.

### 8.9- Fraude con Tarjetas de Crédito en Línea

Delincuentes realizan compras en línea con tarjetas de crédito robadas, aprovechando la facilidad de compra en línea para cometer fraude.

### 8.10 Ataques a la Infraestructura Financiera

Ciberataques dirigidos a instituciones financieras, como bancos y bolsas de valores, buscan robar información confidencial, interrumpir operaciones o causar pérdidas financieras.

## 9. Legislación, marco juridico

Los artículos proporcionados del Código Civil ecuatoriano establecen principios fundamentales sobre la validez y ejecución de los contratos, así como las responsabilidades de las partes involucradas

Código civil Art. 1561 (Ecuador, 2022) - Validez del Contrato: Este artículo destaca la importancia del consentimiento mutuo para la validez de un contrato. En el ámbito de delitos financieros, especialmente aquellos relacionados con fraudes en línea, el consentimiento mutuo puede ser objeto de manipulación mediante técnicas de phishing o engaño digital. La protección legal en estos casos podría requerir una revisión de la validez del contrato en situaciones donde el consentimiento se obtuvo de manera fraudulenta a través de medios tecnológicos.

Código civil Art. 1562 (Ecuador, 2022) - Ejecución de Buena Fe: La obligación de ejecutar los contratos de buena fe es esencial en cualquier transacción, incluyendo aquellas realizadas por medios tecnológicos. En delitos financieros, la mala fe puede manifestarse a través de transacciones fraudulentas en línea. Este principio respalda la necesidad de medidas legales contra aquellos que actúan de manera deshonesta o maliciosa en el ámbito financiero digital.

Código civil Art. 1563 (Ecuador, 2022) - Responsabilidad del Deudor: Este artículo establece la responsabilidad del deudor en función de la naturaleza del

contrato. En delitos financieros, especialmente en el caso de transacciones electrónicas, podría ser relevante para determinar la responsabilidad del deudor en situaciones de fraude en línea, robo de identidad u otras formas de delitos financieros tecnológicos.

Código civil Art. 1564 (Ecuador, 2022) - Obligación de Dar y Conservar: Este artículo establece que la obligación de dar incluye la de entregar la cosa y, si es una especie o cuerpo cierto, la de conservarlo hasta la entrega. En el contexto de delitos financieros tecnológicos, podría relacionarse con la responsabilidad de las instituciones financieras en la protección de la información del cliente y la obligación de salvaguardarla contra posibles amenazas cibernéticas.

Los artículos 1561-1564 del código civil (Ecuador, 2022) nos habla sobre el compromiso que se lleva a cabo en los contratos por otro lado esto cobra relevancia en el momento que se compara con la asociación que nosotros le damos al uso de una tarjeta de crédito, podríamos abogar de que la tarjeta de crédito es un extensor mas de nuestro derecho de voluntad por nuestra parte, y al ser perjudicado por una suplantación de identidad e uso de la tarjeta sin consentimiento estaríamos siendo vulnerado nuestro derecho de voluntad para ejercer tal contrato.

Artículo 212 del COIP (Asambrea Nacional, 2021) de Ecuador, tiene una estrecha relación con los delitos financieros perpetrados mediante el uso de tecnología tales como:

Fraudes en transacciones financieras en línea. - Los delincuentes pueden hacerse pasar por otra persona para acceder a cuentas bancarias, realizar transferencias no autorizadas o llevar a cabo estafas electrónicas.

Phishing e ingeniería social. - Los atacantes pueden utilizar correos electrónicos, mensajes falsos o sitios web fraudulentos para obtener información financiera confidencial al hacerse pasar por entidades legítimas, como instituciones financieras.

Creación de cuentas falsas. - Los delincuentes pueden utilizar identidades robadas para establecer perfiles fraudulentos en plataformas financieras, comprometiendo la seguridad y la confidencialidad de la información del usuario.

Lavado de dinero digital. - Los delincuentes pueden utilizar identidades falsas para realizar transacciones financieras ilícitas y ocultar el origen de los fondos mediante el uso de tecnologías como las criptomonedas.

El Artículo 166 del COIP (Asambrea Nacional, 2021) de Ecuador trata sobre el "Acoso Sexual" puede relacionarse con delitos financieros por medio del uso de tecnologías de la siguiente manera:

Ciberacoso Sexual. - El artículo considera el ciberacoso sexual como una forma de acoso sexual cuando se utiliza tecnología de la información y comunicación. En el contexto financiero, esto podría vincularse a situaciones en las que el acoso se realiza con la intención de obtener beneficios financieros, como chantaje económico o fraude mediante amenazas de revelar información comprometedora.

Amenazas Relacionadas con Legítimas Expectativas. - La amenaza de causar un mal relacionado con las legítimas expectativas en el ámbito de la relación de subordinación puede estar relacionada con delitos financieros. Un agresor que posee información confidencial sobre la víctima podría amenazar con revelar datos financieros sensibles, lo que podría dar lugar a extorsión o actividades fraudulentas.

Menores de Edad y Personas Vulnerables. -La mención de sanciones más severas cuando la víctima es menor de dieciocho años, persona con discapacidad o incapaz de comprender el significado del hecho, destaca la necesidad de proteger a grupos vulnerables. En el ámbito financiero, la vulnerabilidad de estos grupos podría ser explotada para cometer delitos financieros, como el robo de identidad o fraudes en línea.

Vínculos Familiares y Delitos Financieros. - La disposición que sanciona con el máximo de la pena cuando el acoso sexual es cometido por miembros del núcleo familiar o personas con vínculos íntimos destaca la gravedad de estos casos. En el ámbito financiero, esto podría estar relacionado con situaciones de abuso financiero dentro del ámbito familiar, como el acceso no autorizado a cuentas bancarias.

El Artículo 47 del COIP (Asambrea Nacional, 2021) de Ecuador establece circunstancias agravantes de la infracción penal en la cual es vinculante con el

artículo 186 del mismo ordenamiento jurídico el cual trata sobre la estafa y establece sanciones para aquellos que, con el objetivo de obtener un beneficio patrimonial, utilicen simulación de hechos falsos, deformación u ocultamiento de hechos verdaderos para inducir a error a otra persona. Este artículo tiene una clara relevancia en el contexto de delitos financieros por medio de usos tecnológicos. La pena máxima se aplica a diversas modalidades, entre las cuales destaca el uso fraudulento de tarjetas de crédito o débito, así como el empleo de dispositivos electrónicos para alterar cajeros automáticos y capturar información de tarjetas. Además, el artículo contempla sanciones específicas para estafas cometidas a través de instituciones financieras y establece medidas para prevenir fraudes en la venta de valores, operaciones ficticias y creación de compañías ficticias.

## 10. Impacto en la seguridad jurídica

La creciente integración de la tecnología en el ámbito financiero ha generado un impacto significativo en la seguridad jurídica. A medida que las instituciones financieras adoptan soluciones tecnológicas para agilizar procesos y mejorar la eficiencia, surgen desafíos legales relacionados con la protección de la información y la privacidad de los usuarios. El uso de plataformas digitales, servicios en línea y la gestión de grandes cantidades de datos financieros ha suscitado preocupaciones sobre la vulnerabilidad a posibles ciberataques y la necesidad de robustas medidas de seguridad jurídica para salvaguardar la integridad de las transacciones y la confidencialidad de la información financiera.

Además, la rápida evolución de las tecnologías financieras, conocidas como fintech, plantea interrogantes sobre la adaptación de las regulaciones legales existentes a estas innovaciones. La agilidad con la que se desarrollan nuevas herramientas financieras, como blockchain y contratos inteligentes, requiere una revisión constante de los marcos legales para garantizar la protección de los intereses de todas las partes involucradas. La seguridad jurídica en el ámbito financiero, en el contexto tecnológico actual, implica el equilibrio entre fomentar la innovación y salvaguardar los derechos y la confianza de los participantes en el

sistema financiero, haciendo hincapié en la necesidad de un marco legal que evolucione de manera paralela al avance tecnológico.

## 11. Identificación de desafíos y riesgos jurídicos asociados al uso de tecnología en la comisión de delitos financieros

El avance tecnológico ha introducido nuevos desafíos y riesgos en la comisión de delitos financieros. La identificación de estos desafíos implica reconocer amenazas como el phishing, malware, y ataques de ransomware, que buscan explotar vulnerabilidades en sistemas financieros. Además, la rápida adopción de criptomonedas ha introducido desafíos específicos, como el lavado de dinero digital y el anonimato asociado con las transacciones en monedas virtuales. El riesgo de ingeniería social, donde los delincuentes utilizan tácticas psicológicas para obtener información confidencial, también se ha intensificado con la mayor interconexión digital. La identificación de estos desafíos requiere una comprensión profunda de las tecnologías involucradas y su potencial para el uso malintencionado.

## 12.Evaluación De Las Respuestas Institucionales Y Jurídicas Ante Estos Desafíos

Las respuestas institucionales y jurídicas ante los desafíos tecnológicos en delitos financieros deben ser proactivas y adaptarse a la evolución constante de las amenazas. Esto implica el fortalecimiento de regulaciones financieras para abordar específicamente los delitos en línea, así como la implementación de medidas de seguridad cibernética en las instituciones financieras. La colaboración entre gobiernos, fuerzas del orden y entidades financieras es crucial para compartir información y desarrollar estrategias efectivas. Además, la educación y concienciación sobre ciberseguridad son esenciales para empoderar a los usuarios y reducir el riesgo de caer en actividades delictivas en línea. La adopción de tecnologías de análisis de datos y monitoreo constante puede fortalecer las respuestas institucionales para detectar y prevenir delitos financieros en un entorno digital en constante cambio.

## 13. Buenas Prácticas Y Medidas De Prevención

Educación y Concientización. - Implementar programas de educación para empleados y usuarios finales sobre los riesgos asociados con delitos financieros en línea. Asegurarse de que comprendan las tácticas de phishing, ingeniería social y otras amenazas cibernéticas.

Actualización Continua. -Mantener actualizados los sistemas y software con las últimas actualizaciones de seguridad. Los parches de seguridad y las actualizaciones regulares pueden cerrar las vulnerabilidades que los delincuentes podrían explotar.

Autenticación de Dos Factores (2FA). - Implementar la autenticación de dos factores en todas las transacciones financieras en línea y en el acceso a plataformas financieras. Esto agrega una capa adicional de seguridad al requerir una segunda forma de autenticación.

Monitoreo de Transacciones. - Establecer sistemas de monitoreo de transacciones para detectar patrones inusuales o actividades sospechosas. Los algoritmos de aprendizaje automático pueden ser efectivos para identificar anomalías en grandes conjuntos de datos financieros.

Encriptación de Datos. - Utilizar encriptación fuerte para proteger la información financiera tanto en reposo como en tránsito. Esto incluye datos almacenados en servidores, así como información transmitida a través de redes.

Políticas de Acceso y Control. - Establecer políticas estrictas de acceso y control de privilegios para limitar quién puede acceder a la información financiera sensible. Monitorear y auditar regularmente el acceso a sistemas críticos.

Auditorías de Seguridad. -Realizar auditorías de seguridad de manera regular para identificar y abordar posibles debilidades en los sistemas. Contratar a expertos en seguridad cibernética para evaluar la infraestructura y proponer mejoras.

Colaboración con Autoridades. - Mantener una estrecha colaboración con las autoridades legales y de aplicación de la ley para informar sobre actividades sospechosas y facilitar investigaciones rápidas.

Protección contra Ransomware. - Implementar medidas de seguridad avanzadas para protegerse contra ataques de ransomware, como copias de seguridad regulares y la concienciación del personal sobre los riesgos asociados.

Evaluación de Proveedores. - Realizar una debida diligencia exhaustiva al seleccionar proveedores de servicios financieros y plataformas tecnológicas. Asegurarse de que cumplan con estándares de seguridad reconocidos y regulaciones pertinentes.

## 14. Estrategias Globales Para La Prevención De Este Tipo De Delitos

varias estrategias clave que han demostrado ser efectivas en el ámbito global. En primer lugar, la implementación de programas integrales de debida diligencia y conocimiento del cliente (KYC) es esencial. Esto incluye la verificación exhaustiva de la identidad de los clientes y la monitorización constante de las transacciones para detectar patrones inusuales.

KYC −know your costumer o conozca a su cliente− que permite confirmar que un cliente es quien dice ser, antes y durante el tiempo que haga negocios y utilice los productos de una institución financiera. Cada cliente debe enviar documentos que certifiquen su identidad y dirección de residencia, algunos ejemplos de este tipo de credenciales, además de los papeles mencionados, son la verificación facial y biométrica (Arango, 2022).

Además, la promoción de una cultura organizacional de cumplimiento y ética es fundamental. Las instituciones financieras deben fomentar la conciencia sobre los

riesgos de delitos financieros entre su personal, proporcionando capacitación regular y estableciendo políticas claras en línea con estándares internacionales.

La colaboración entre instituciones financieras, organismos gubernamentales y autoridades reguladoras es otra práctica crucial. El intercambio de información y la coordinación eficiente fortalecen la capacidad para identificar y abordar posibles amenazas de manera proactiva. Asimismo, la implementación de tecnologías avanzadas, como análisis de datos y inteligencia artificial, puede mejorar la capacidad predictiva y la detección temprana de actividades sospechosas.

Por último, la actualización constante de regulaciones y el fortalecimiento de medidas de cumplimiento son esenciales para adaptarse a la evolución de las amenazas. Las instituciones financieras y los gobiernos deben revisar y mejorar continuamente sus marcos legales y regulaciones para mantenerse a la vanguardia en la lucha contra los delitos financieros a nivel internacional.

## 15. Estrategias Preventivas Que Pueden Ser Implementadas En Guayaquil

### 15.1- fortalecimiento de la Regulación Financiera Local

Revisar y actualizar la legislación local para abordar específicamente los delitos financieros en el entorno digital.

Colaborar con expertos legales y tecnológicos para adaptar la normativa a las amenazas emergentes, incluyendo el uso de criptomonedas.

### 15.2- Capacitación y Concientización

Desarrollar programas de capacitación específicos para el personal de instituciones financieras, así como para usuarios finales, destacando las tácticas de phishing y otras amenazas cibernéticas comunes.

Colaborar con entidades educativas y empresas para difundir información sobre seguridad financiera digital.

### 15.3- Establecimiento de Centros de Respuesta Rápida

Crear centros especializados para responder rápidamente a incidentes de seguridad cibernética, facilitando la colaboración entre instituciones financieras, autoridades gubernamentales y fuerzas del orden locales.

### 15.4- Incentivar la Implementación de Tecnologías de Seguridad

Ofrecer incentivos fiscales o beneficios a instituciones financieras que adopten tecnologías avanzadas de seguridad, como sistemas de autenticación robustos y soluciones de monitoreo de transacciones en tiempo real.

### 15.5- Fomentar la Colaboración Público-Privada

Establecer grupos de trabajo conjuntos entre el sector público y privado para intercambiar información, identificar amenazas emergentes y desarrollar estrategias de prevención efectivas.

### 15.6- Monitoreo Activo de Actividades Financieras

Implementar sistemas de monitoreo activo de transacciones y comportamientos financieros para detectar patrones inusuales y actividades sospechosas, con un enfoque especial en el uso de nuevas tecnologías como blockchain.

### 15.7- Desarrollo de una Plataforma de Denuncias en Línea

Establecer una plataforma en línea para que los ciudadanos y las empresas puedan informar de manera segura y rápida cualquier actividad sospechosa, facilitando la participación activa de la comunidad en la prevención de delitos financieros.

### 15.8- Promoción de Prácticas de Ciberseguridad en Empresas

Trabajar con asociaciones empresariales para fomentar la adopción de mejores prácticas de ciberseguridad en las empresas, especialmente en aquellas que manejan información financiera sensible.

### 15.9- Participación en Redes Internacionales de Seguridad Financiera

Colaborar con organismos internacionales y participar en redes de intercambio de información para mantenerse actualizado sobre las tendencias globales en delitos financieros y compartir mejores prácticas.

### 15.10- Fomentar el Uso Responsable de Criptomonedas

Educar a los ciudadanos y empresas sobre el uso seguro y responsable de criptomonedas, implementando regulaciones que promuevan la transparencia y la legalidad en las transacciones digitales.

## 16. Conclusión

En virtud de la hipótesis planteada y los objetivos de investigación delineados, se evidencia la compleja intersección entre el uso de la tecnología en la comisión de delitos financieros y sus impactos en la seguridad jurídica y la estabilidad económica en Guayaquil. La hipótesis destaca las barreras legales y operativas que subyacen en la regulación de los delitos financieros en el ámbito digital, destacando lagunas normativas, la falta de adaptación legal a la evolución tecnológica, las limitaciones institucionales para enfrentar amenazas digitales y la complejidad transfronteriza de estos delitos.

El análisis de los objetivos de investigación revela la necesidad urgente de abordar las deficiencias actuales en la regulación de los delitos financieros en el entorno digital en Guayaquil. Además, se resalta la importancia de comprender el impacto económico y social de estos delitos en la seguridad jurídica y la estabilidad económica de la región. La identificación de medidas efectivas para fortalecer la protección y prevención de delitos financieros en la economía digital emerge como un imperativo, sugiriendo la implementación de estrategias que incluyan la actualización y fortalecimiento de la legislación, la promoción de la colaboración internacional y el impulso de capacidades tecnológicas en las instituciones pertinentes.

En este contexto, la investigación propuesta se presenta como un paso crucial hacia la comprensión profunda de los desafíos actuales y la formulación de soluciones prácticas para salvaguardar la seguridad jurídica y la estabilidad

económica de Guayaquil en la era digital, contribuyendo así al fortalecimiento de la resiliencia del sistema financiero frente a las amenazas emergentes.

## CAPITULO II
## METODOLOGIA DE LA INVESTIGACION

El enfoque de investigación utilizado fue el cuantitativo de tipo no experimental transversal de alcance descriptivo. Se utilizó una encuesta como instrumento para recolectar datos sobre el impacto en la seguridad jurídica sobre la regulación de los delitos financieros en la economía digital de Guayaquil.

La investigación descriptiva o método descriptivo de investigación es el procedimiento usado en ciencia para describir las características del fenómeno, sujeto o población a estudiar. Al contrario que el método analítico, no describe

por qué ocurre un fenómeno, sino que se limita a observar lo que ocurre sin buscar una explicación (Martinez , 2018).

El enfoque descriptivo permitirá examinar exhaustivamente cómo la tecnología ha sido utilizada por individuos malintencionados para llevar a cabo delitos financieros, tales como fraudes bancarios, estafas en línea y lavado de dinero. Además, se analizará cómo las instituciones jurídicas y de seguridad en Guayaquil han respondido a estos desafíos, implementando medidas tecnológicas y legales para salvaguardar la seguridad financiera y jurídica en la región.

A través de la investigación descriptiva, se podrán identificar patrones, tendencias y posibles brechas en la seguridad jurídica relacionadas con el uso de la tecnología en la comisión de delitos financieros. Esto no solo permitirá una comprensión más profunda de la problemática, sino que también proporcionará una base sólida para la formulación de estrategias y políticas que fortalezcan la seguridad jurídica en un entorno cada vez más tecnológico y cambiante.

La población utilizada fue la carrea de Derecho y gobernabilidad de la Universidad Ecotec. La tipo de muestra fue enfocada o dirigida, porque consistió en seleccionar a un grupo determinado con características oportunas para el estudio, esto es, un grupo que maneja el tema de interés, con una opinión técnica.

**Técnicas e Instrumentos**

**Encuesta**

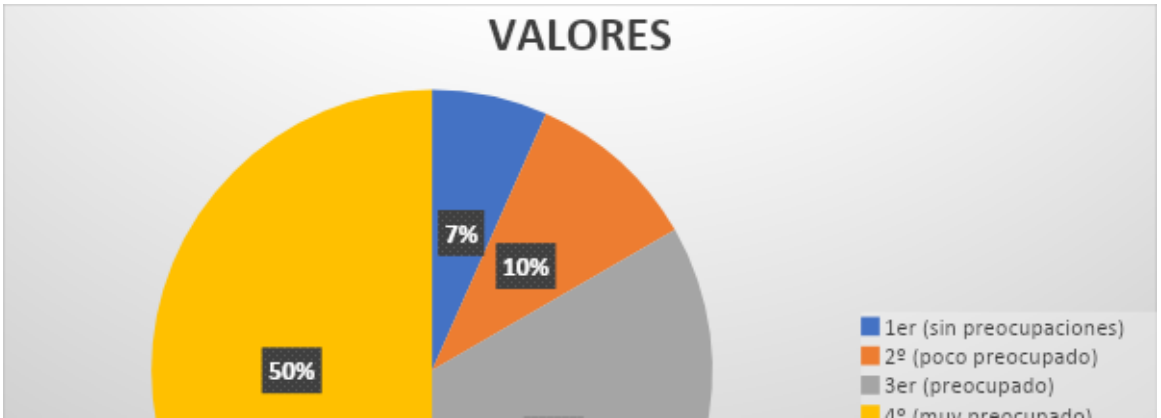
Se realizó mediante un cuestionario conformado por quince preguntas que giran en torno a la problemática analizada, mediante el cual se obtuvieron opiniones objetivas emitidas por treinta personas cuyas personas pertenecen a la Facultad de Derecho y Gobernabilidad de la Universidad Ecotec los cuales conocen parte del tema dado a que se forman em base a el estudio de las

leyes, a continuación, se detallan las preguntan las cuales conforman la encuesta:

¿Qué tan preocupado/a está por la posibilidad de ser víctima de fraudes en transacciones financieras en línea?, En su opinión, ¿las medidas legales actuales son suficientes para abordar los delitos financieros tecnológicos?, ¿Cuál es su percepción sobre la efectividad de las instituciones financieras en la protección de la información del cliente contra amenazas cibernéticas?, En relación con el uso de tarjetas de crédito, ¿cree que las tecnologías actuales ofrecen suficiente seguridad para prevenir fraudes?, ¿Cuán consciente se siente de los riesgos asociados con el phishing e ingeniería social en transacciones financieras en línea?, ¿Considera que la legislación debería imponer sanciones más severas para los delitos financieros tecnológicos que involucren la creación de cuentas falsas?, En su opinión, ¿el ciberacoso sexual debería ser considerado como una forma de acoso sexual, especialmente cuando se busca obtener beneficios financieros?, ¿Cuánto cree que las amenazas relacionadas con legítimas expectativas podrían estar vinculadas con delitos financieros?, ¿Cree que las sanciones más severas para delitos financieros contra menores de edad y personas vulnerables son necesarias para proteger a estos grupos?, ¿En qué medida cree que la vulnerabilidad de menores de edad y personas con discapacidad es explotada para cometer delitos financieros?, ¿Considera que las tecnologías como las criptomonedas están contribuyendo al aumento del lavado de dinero digital?, En relación con la estafa y el uso fraudulento de tarjetas de crédito, ¿cree que las penas establecidas por la legislación son proporcionales a la gravedad de estos delitos?, ¿Cuál es su percepción sobre la eficacia de las medidas para prevenir fraudes en la venta de valores y operaciones ficticias según la legislación actual?, ¿Cree que las instituciones financieras deberían asumir una mayor responsabilidad en la protección de la información del cliente en el contexto de delitos financieros tecnológicos?, En su experiencia o conocimiento, ¿cree que el uso de tecnologías ha aumentado la sofisticación de los delitos financieros?

## CAPITULO III
## ANALISIS DE RESULTADOS

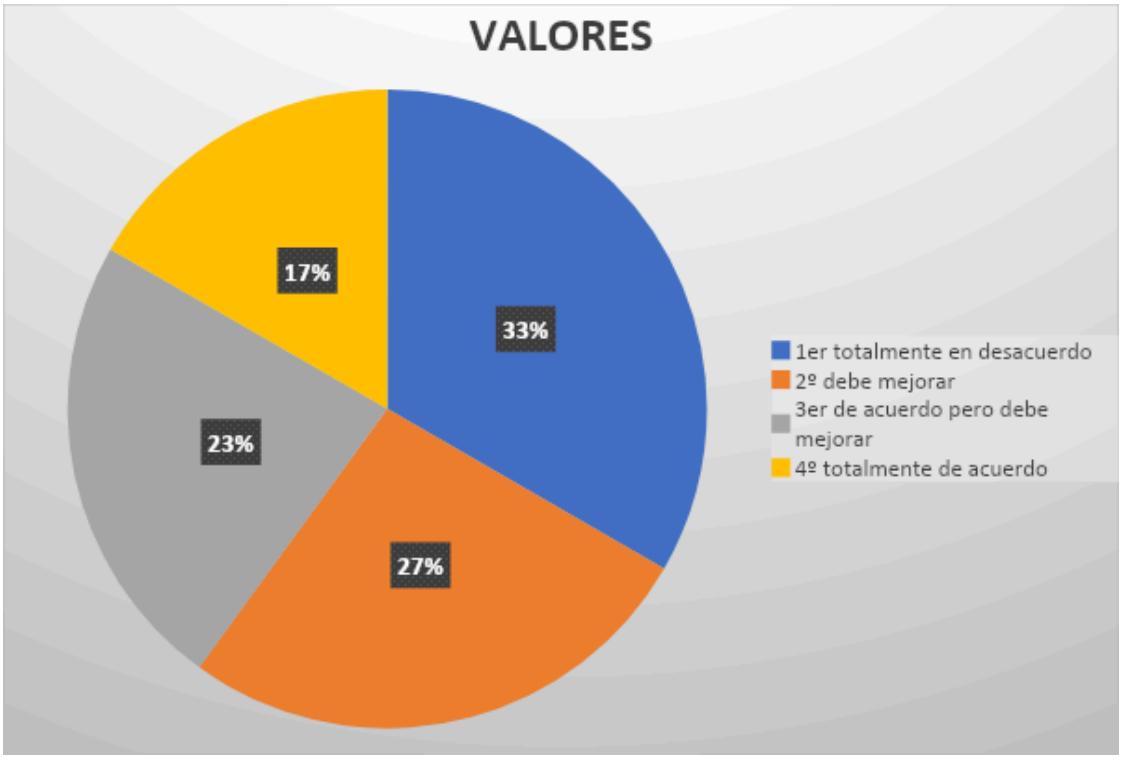
**1.**- ¿Qué tan preocupado/a está por la posibilidad de ser víctima de fraudes en transacciones financieras en línea?



**Análisis**

Un total de 25 de 30 personas (83.3%) están de acuerdo o totalmente de acuerdo en que están preocupadas por ser víctimas de fraudes en transacciones financieras en línea. Esto sugiere que existe una alta conciencia y preocupación sobre los riesgos de seguridad en línea

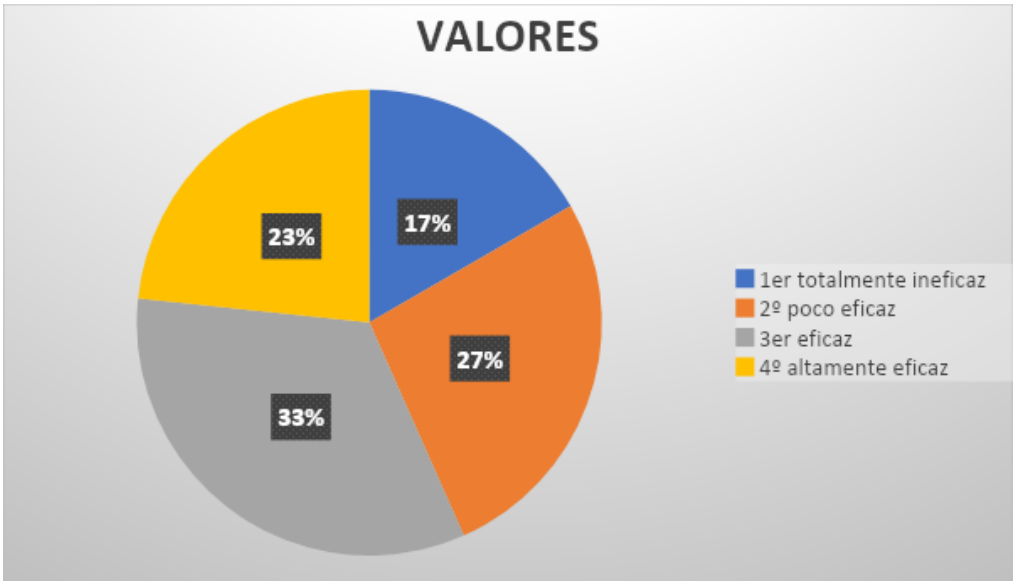
**2.-** En su opinión, ¿las medidas legales actuales son suficientes para abordar los delitos financieros tecnológicos?




**Análisis**

Un total de 18 de 30 personas (60%) están en desacuerdo o totalmente en desacuerdo en que las medidas legales actuales son suficientes para abordar los delitos financieros tecnológicos. Esto indica una percepción generalizada de que las leyes y regulaciones actuales pueden no ser suficientes para combatir eficazmente los delitos financieros en línea.

**3**.- ¿Cuál es su percepción sobre la efectividad de las instituciones financieras en la protección de la información del cliente contra amenazas cibernéticas?




**Análisis**

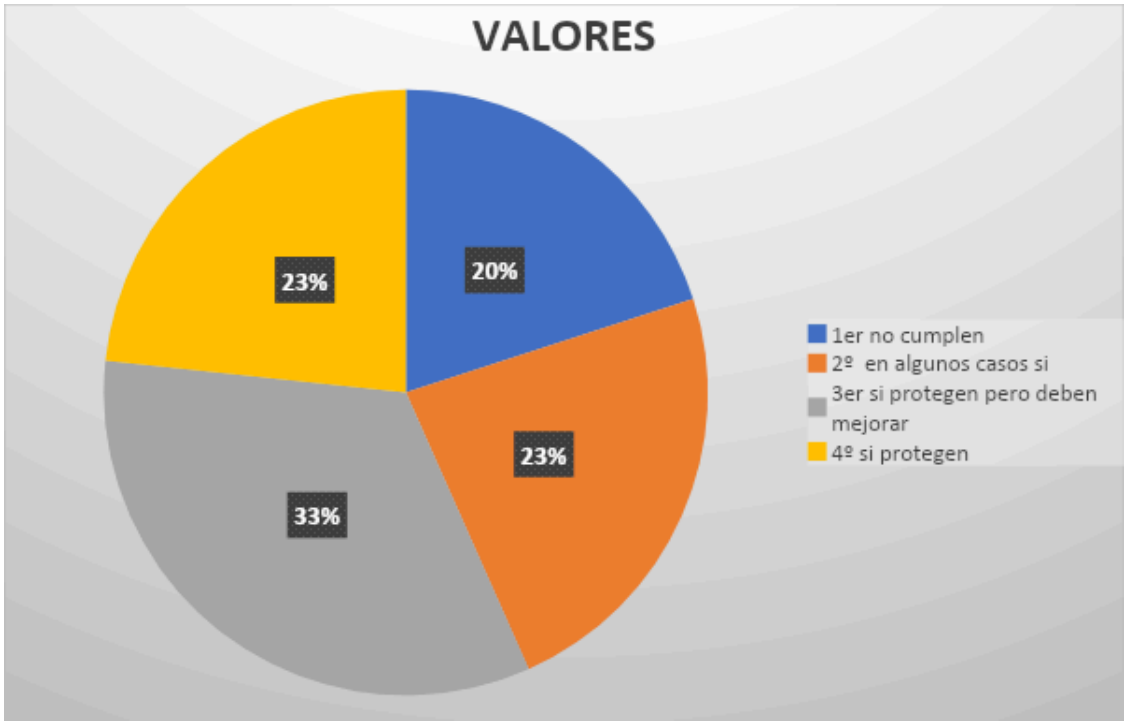
Las opiniones sobre la efectividad de las instituciones financieras en la protección de la información del cliente contra amenazas cibernéticas están divididas, con 17 de 30 personas (56.7%) creyendo que son eficaces o altamente eficaces, y 13 de 30 personas (43.3%) creyendo que son poco eficaces o totalmente ineficaces. Esto sugiere que hay una variabilidad significativa en la percepción de la eficacia de las instituciones financieras en este aspecto.

Talvez la poca explicación o vaga explicación que dan estas instituciones financieras sobre sus actos contra los delitos cibernéticos y los actos que cometen para ir en contra de estos delitos no están debidamente explicada o de libre acceso a esta información para un público más informal o que no esté muy enterado de estos temas

La poca o casi inexistente investigación hecha por el público general de las cuales estas instituciones se benefician, son el arca perfecta para la poca implementación de actitudes en contra de los delitos financieros ya que el público general al no estar muy enterado de estos temas sienten que hay un desequilibrio

entre las defensas y amenazas que suponen este tipo de delitos en contra de su patrimonio, el cual hace que el propio publico sea más precavido y le quite un gran peso a las instituciones financieras

**4**.-En relación con el uso de tarjetas de crédito, ¿cree que las tecnologías actuales ofrecen suficiente seguridad para prevenir fraudes?




**Análisis**

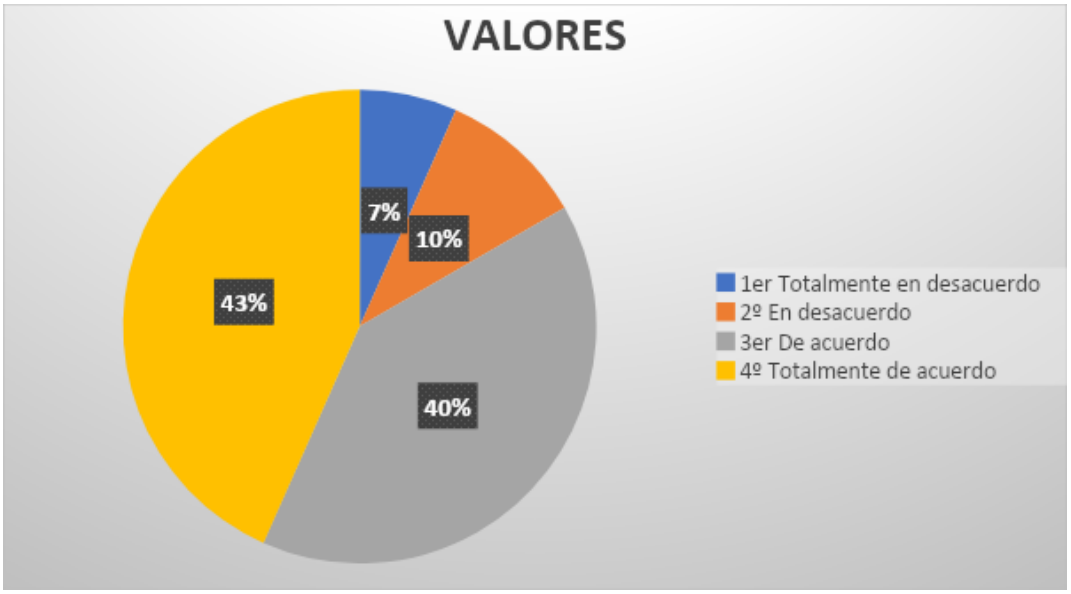
Un total de 17 de 30 personas (56.7%) están de acuerdo o totalmente de acuerdo en que las tecnologías actuales ofrecen suficiente seguridad para prevenir fraudes con tarjetas de crédito. Esto indica una confianza moderada en las medidas de seguridad actuales.

**5.**-¿Cuán consciente se siente de los riesgos asociados con el phishing e ingeniería social en transacciones financieras en línea?

**Análisis**

Un total de 22 de 30 personas (73.3%) se sienten conscientes o muy conscientes de los riesgos asociados con el phishing e ingeniería social en transacciones financieras en línea. Esto sugiere que la mayoría de las personas están bien informadas sobre estos riesgos específicos.

**6.**- ¿Considera que la legislación debería imponer sanciones más severas para los delitos financieros tecnológicos que involucren la creación de cuentas falsas?




**Análisis**

Un total de 25 de 30 personas (83.3%) están de acuerdo o totalmente de acuerdo en que la legislación debería imponer sanciones más severas para los delitos financieros tecnológicos que involucren la creación de cuentas falsas. Esto indica un fuerte apoyo para medidas legales más estrictas en este aspecto.

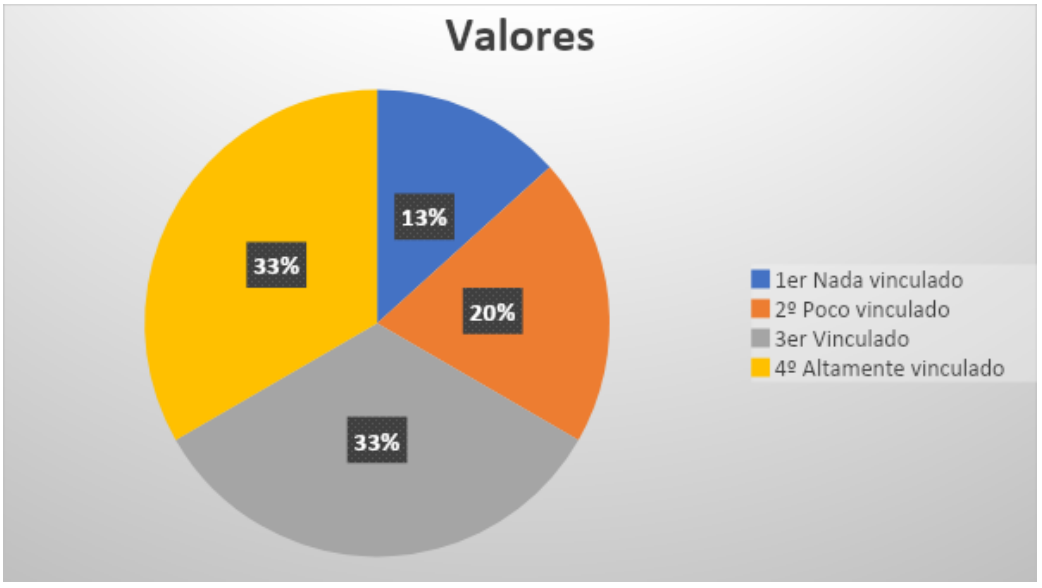
**7**.-En su opinión, ¿el ciberacoso sexual debería ser considerado como una forma de acoso sexual, especialmente cuando se busca obtener beneficios financieros?

**Análisis**

Un total de 27 de 30 personas (90%) están de acuerdo o totalmente de acuerdo en que el ciberacoso sexual debería ser considerado como una forma de acoso sexual. Esto indica un reconocimiento casi unánime de la gravedad de este problema.

En este punto la gran mayoría estuvo de acuerdo con esta opinión, la cual hace una máscara de las sociedad ecuatoriana la cual tiene muy presente el problema que tiene, el cual es el acoso sexual el cual cada año va aumentando con la facilidad que se puede llegar a cometer aprovechándose de la confianza de personas que cada vez es más frecuente que sea cometido hacia el género femenino y con rasgos de tendencia hacia las menores de edad, por medio de chantajes y extorciones las cuales las víctimas aceptan cualquier cosa con tal de no ser expuesto su contenido en las redes sociales

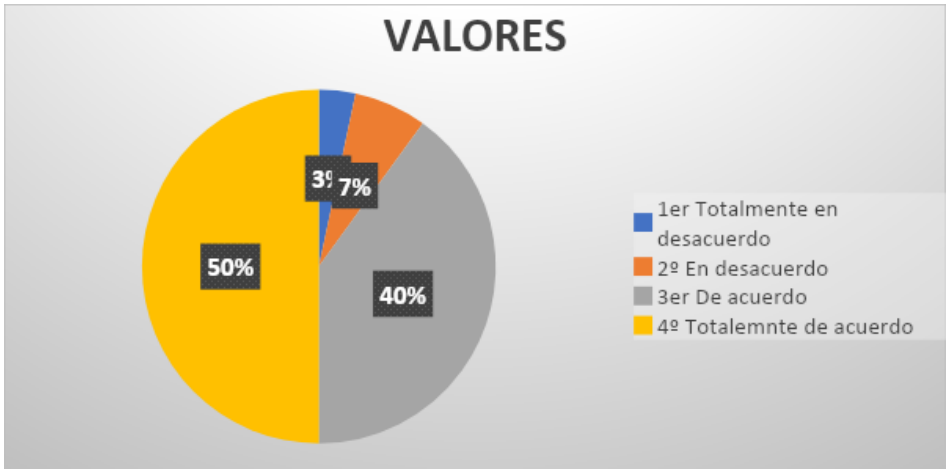
**8.**- ¿Cuánto cree que las amenazas relacionadas con legítimas expectativas podrían estar vinculadas con delitos financieros?




**Análisis**

Las opiniones sobre cuánto las amenazas relacionadas con legítimas expectativas podrían estar vinculadas con delitos financieros están divididas, con 20 de 30 personas (66.7%) creyendo que están vinculadas o altamente vinculadas, y 10 de 30 personas (33.3%) creyendo que están poco vinculadas o nada vinculadas. Esto sugiere que este es un área que puede requerir más investigación y concienciación.

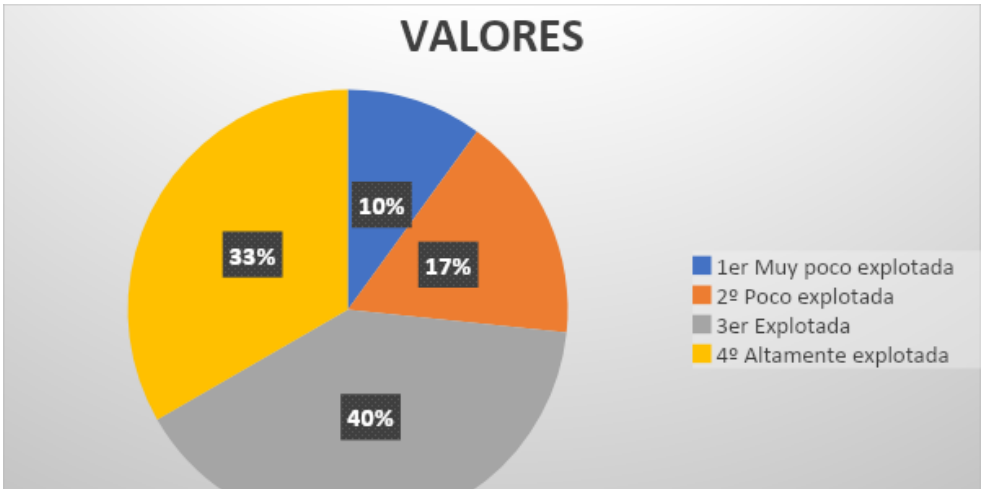
**9**.- ¿Cree que las sanciones más severas para delitos financieros contra menores de edad y personas vulnerables son necesarias para proteger a estos grupos?




**Análisis**

Un total de 27 de 30 personas (90%) están de acuerdo o totalmente de acuerdo en que se necesitan sanciones más severas para delitos financieros contra menores de edad y personas vulnerables para proteger a estos grupos. Esto indica un fuerte apoyo para medidas de protección más fuertes para estos grupos vulnerables.

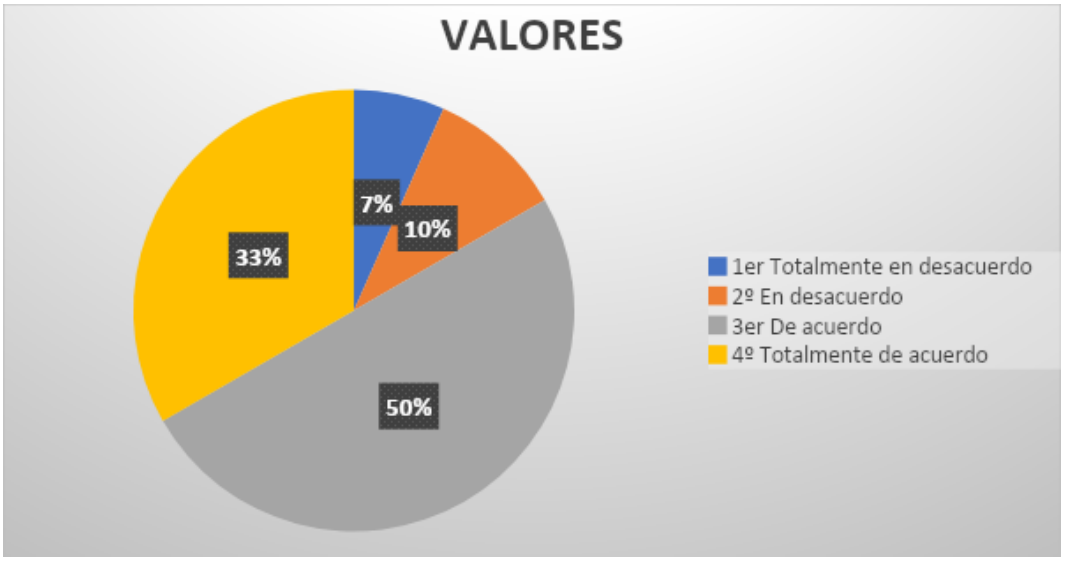
**10.-¿**En qué medida cree que la vulnerabilidad de menores de edad y personas con discapacidad es explotada para cometer delitos financieros?



**Análisis**

Las opiniones sobre en qué medida la vulnerabilidad de menores de edad y personas con discapacidad es explotada para cometer delitos financieros están divididas, con 22 de 30 personas (73.3%) creyendo que está explotada o altamente explotada, y 8 de 30 personas (26.7%) creyendo que está poco explotada o muy poco explotada. Esto sugiere que este es un área que puede requerir más investigación y concienciación.

**11.**-¿Considera que las tecnologías como las criptomonedas están contribuyendo al aumento del lavado de dinero digital?



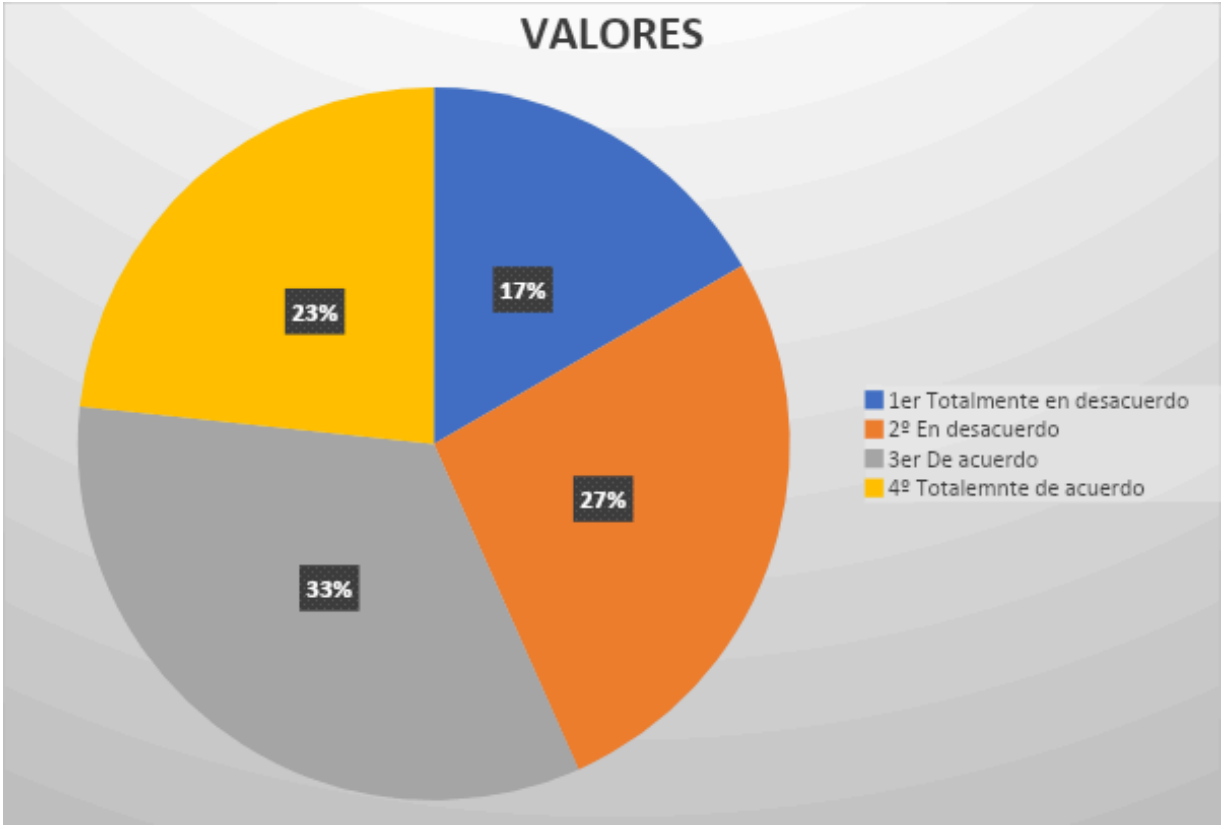

**Análisis**

Un total de 25 de 30 personas (83.3%) están de acuerdo o totalmente de acuerdo en que las tecnologías como las criptomonedas están contribuyendo al

aumento del lavado de dinero digital. Esto indica una conciencia generalizada de los riesgos asociados con estas tecnologías.

Si bien las criptomonedas en estos últimos años han obtenido una gran popularidad gracias a muchas personas influyentes las cuales las usan dándoles más fama a este nuevo estilo de moneda virtual la realidad es que es una moneda que está en fluctuación contante por lo cual su valor varia constantemente lo cual hace que muchas personas quieran aprovecharse del desconocimiento de las personas y realizan estafas piramidales por medio de tradings el cual juegan con el sueño de las personas de querer ser millonarias solo robándole todo su dinero por medio de farsas

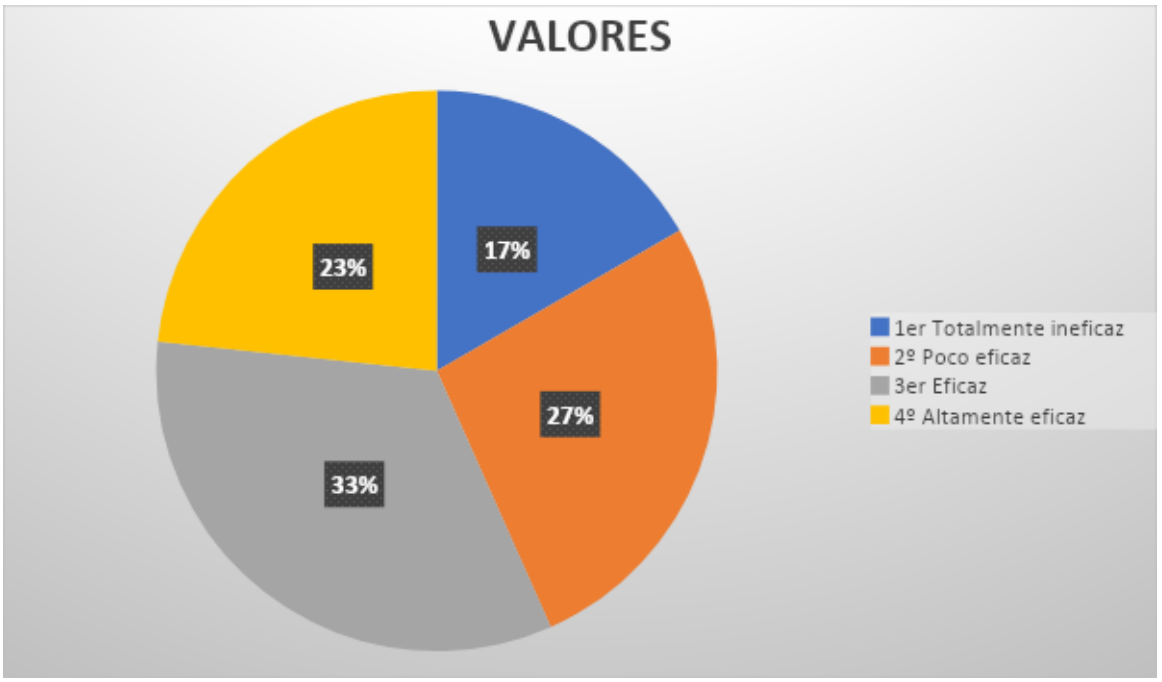
**12.**-En relación con la estafa y el uso fraudulento de tarjetas de crédito, ¿cree que las penas establecidas por la legislación son proporcionales a la gravedad de estos delitos?




**Análisis**

Las opiniones sobre si las penas establecidas por la legislación son proporcionales a la gravedad de la estafa y el uso fraudulento de tarjetas de crédito están divididas, con 17 de 30 personas (56.7%) creyendo que están de acuerdo o totalmente de acuerdo, y 13 de 30 personas (43.3%) creyendo que están en desacuerdo o totalmente en desacuerdo. Esto sugiere que puede haber un debate en curso sobre este tema.

**13.**-¿Cuál es su percepción sobre la eficacia de las medidas para prevenir fraudes en la venta de valores y operaciones ficticias según la legislación actual?



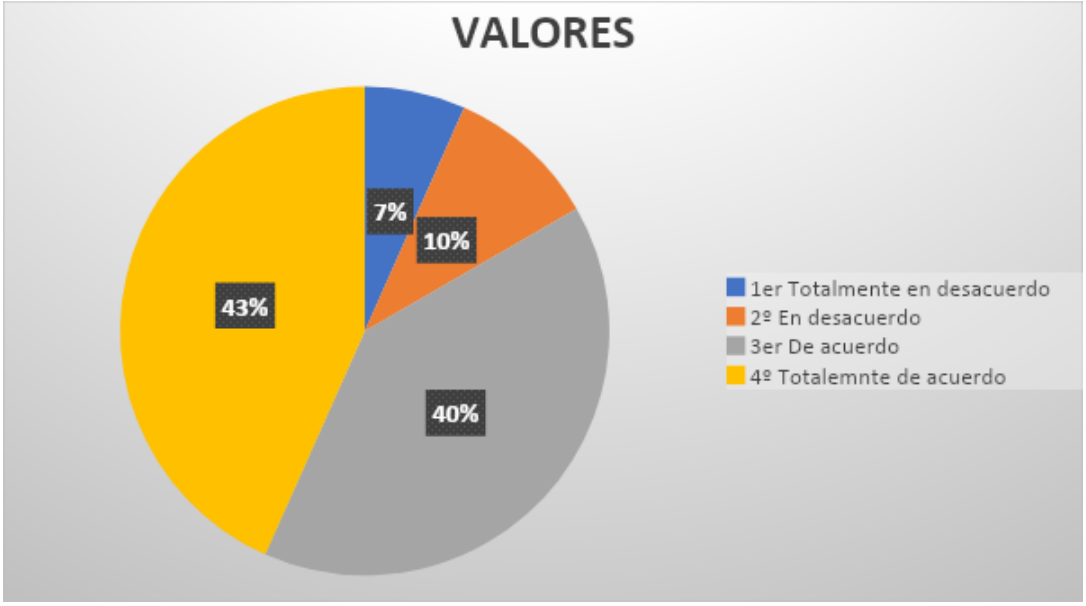

**Análisis**

Las opiniones sobre la eficacia de las medidas para prevenir fraudes en la venta de valores y operaciones ficticias según la legislación actual están divididas, con 17 de 30 personas (56.7%) creyendo que son eficaces o altamente eficaces, y 13 de 30 personas (43.3%) creyendo que son poco eficaces o totalmente ineficaces. Esto sugiere que este es un área que puede requerir más investigación y concienciación.

Las opiniones en esta pregunta fueron muy parejas, pero cabe destacar que en el Ecuador es común recibir noticias sobre fraudes cometidos por la misma compañía, Este tipo de fraude ocurre cuando un oficial o director de una empresa no reporta de manera precisa la información financiera de la compañía a sus

accionistas1. Esta situación puede hacer que el valor de las acciones de la empresa suba de forma artificial y anime a los inversionistas a comprar acciones de una compañía en problemas (Caval , 2021)

**14.**- ¿Cree que las instituciones financieras deberían asumir una mayor responsabilidad en la protección de la información del cliente en el contexto de delitos financieros tecnológicos?



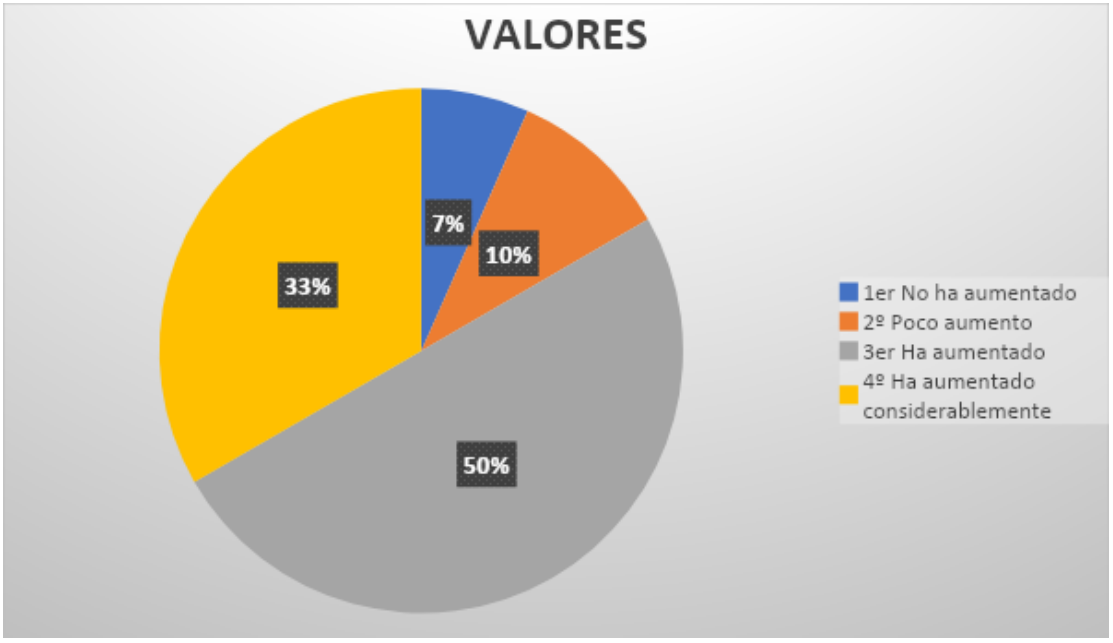

**Análisis**

Un total de 25 de 30 personas (83.3%) están de acuerdo o totalmente de acuerdo en que las instituciones financieras deberían asumir una mayor responsabilidad en la protección de la información del cliente en el contexto de delitos financieros tecnológicos. Esto indica un fuerte apoyo para una mayor responsabilidad corporativa en este aspecto.

La mayoría de personas se sienten indignadas por el aumento de los delitos financieros tecnológicos, con el avance de la tecnología, los delitos financieros también han evolucionado. Los delincuentes utilizan tecnologías avanzadas para cometer fraudes y robar información. Esto incluye delitos como la clonación de

tarjetas de crédito, la suplantación de identidad, el fraude en línea, entre otros (POLICIA NACIONAL DEL ECUADOR , 2015). Dado este aumento, es esencial que las instituciones financieras asuman una mayor responsabilidad en la protección de la información del cliente.

**15.**-En su experiencia o conocimiento, ¿cree que el uso de tecnologías ha aumentado la sofisticación de los delitos financieros?




**Análisis**

Un total de 25 de 30 personas (83.3%) creen que el uso de tecnologías ha aumentado o ha aumentado significativamente la sofisticación de los delitos financieros. Esto indica una conciencia generalizada de cómo la tecnología puede ser utilizada para fines malintencionados.

## CAPÍTULO IV
## PROPUESTA

Los delitos financieros en el entorno digital más común en la ciudad de Guayaquil están las transacciones de compra y venta por medio de redes sociales, páginas webs y tiendas online. Estas interacciones al no ser monitoreadas por una organización legal las hace propensas a que se cometan muchos delitos. De esta forma, a continuación, se detallan 3 aspectos importantes y más comunes.

1.-La libertad para emprender cualquier negocio por medio online puede generar una mayor cantidad de estafas, porque se generan perfiles que no están certificadas por ningún organismo que las acredite.

2.-La ingenuidad de los ciudadanos para comprar productos o servicios por medios online sin tener un proceso riguroso de verificación sobre el perfil del vendedor, es decir, poder confiar en la identidad del vendedor siempre que el comprador lo conozca personalmente o que un organismo Acreditado lo respalde.

3.-La confianza que algunos courier tienen en sus clientes pueden llevarlos a cometer errores como no verificar en todos los momentos los pedidos realizados. En consecuencia, en estos paquetes pueden transitar objetos ilegales como armamentos o estupefacientes, convirtiendo al courier en cómplice o en el menor de los casos pagar multas altas en la aduana.

Entre las medidas efectivas propuestas tenemos:

1.- Que se realice una regulación de los medios virtuales como páginas webs, redes sociales y tiendas virtuales con certificados que aseguren la confianza de los compradores

2.- Que los courier usen un protocolo de seguridad para que ellos sean los que rectifiquen los pedidos

Estas dos medidas de seguridad van permitir que haya un mayor tráfico de oferta y demanda mejorando la economía en el país y también la confianza del ciudadano en la utilidad de los procesos económicos por canales virtuales.

## RECOMENDACIÓN

Después de haber desarrollado la investigación y analizar los puntos flojos que pueden tener el desconocimiento del manejo de información personal utilizada por instituciones financieras, como primer punto se debería llevar a cabo medidas preventivas las cuales sean fáciles de llevar a cabo tanto para las instituciones ya que se implementaría métodos ya existentes los cuales ya detallaré, como también sería fácil de uso para el publico general, hay que recordar que muchas personas ajenas al uso de la tecnología son usuarios de cuentas bancarias las cuales piden ayuda sus hijos y familiares para hacer sus movimientos bancarios y teniendo en cuenta a estas personas estarían los siguientes puntos a desarrollar:

**Educación y Concienciación:** Las campañas de concienciación pueden ser una herramienta efectiva para educar al público sobre los riesgos asociados con los delitos financieros. Estas campañas pueden tomar la forma de talleres, seminarios web, folletos informativos, y más. El objetivo es proporcionar a las personas las herramientas necesarias para reconocer y evitar posibles amenazas.

**Autenticación de Doble Factor**: Esta es una medida de seguridad que requiere que los usuarios proporcionen dos formas de identificación antes de poder acceder a sus cuentas. Por ejemplo, además de ingresar una contraseña, también podrían tener que ingresar un código enviado a su teléfono móvil. Esto

hace que sea mucho más difícil para los delincuentes acceder a las cuentas de las personas.

**Monitoreo Continuo**: Las instituciones financieras pueden implementar sistemas que monitorean constantemente las transacciones y actividades en busca de comportamientos sospechosos. Si se detecta algo inusual, el sistema puede alertar a los responsables de seguridad para que puedan investigar más a fondo.

**Actualizaciones Regulares de Seguridad**: Mantener todos los sistemas y software actualizados es crucial para protegerse contra los delitos financieros. Los ciberdelincuentes a menudo explotan vulnerabilidades en software desactualizado, por lo que es importante instalar regularmente las últimas actualizaciones de seguridad.

**Cooperación con las Autoridades**: Las instituciones financieras deben trabajar en estrecha colaboración con las autoridades locales y nacionales para informar de cualquier actividad sospechosa. Esto puede ayudar a las autoridades a identificar y detener a los delincuentes más rápidamente.

**Cifrado de Datos**: El cifrado convierte los datos en un código que sólo puede ser descifrado con una clave especial. Al cifrar los datos financieros, las instituciones pueden protegerlos de los ciberdelincuentes, incluso si logran acceder a sus sistemas.

También en un punto de la investigación se toco el tema de blockchain o bloqueo de cadena es una codificación la cual a día de hoy es la mas segura de llevar a cabo ya que usa una cadena de encriptación continua la cual hace que la IP de información cambien constantemente siendo casi impenetrables lo cual las hace muy seguras.

**Planes de Respuesta a Incidentes**: En caso de que se produzca un delito financiero, es importante tener un plan de respuesta a incidentes. Este plan debe detallar exactamente qué pasos debe seguir la institución para mitigar el daño, investigar el incidente y recuperarse de él.

Cabe destacar que para la implementación de estos puntos se necesita que el usuario común este más familiarizado con la tecnología al menos para lo más básico y que conozca los riesgos que corre su patrimonio por lo cual es importante también proponer una mejor educación y concienciación sobre los delitos que pueden ser desarrollados por usos tecnológicos por lo cual recomiendo que se lleven a cabo los siguientes puntos para que sea una base sobre la cual trabajar con el usuario promedio los cuales son:

**Talleres y Seminarios**: Las instituciones financieras podrían organizar talleres y seminarios para sus empleados y clientes. Estos eventos podrían cubrir una variedad de temas, como cómo reconocer las señales de un posible delito financiero, qué hacer si se sospecha de un delito y cómo protegerse contra estos delitos.

**Materiales Educativos**: Las instituciones financieras podrían proporcionar a sus clientes materiales educativos sobre delitos financieros. Estos podrían incluir folletos, guías y videos que explican qué son los delitos financieros, cómo ocurren y cómo prevenirlos.

**Campañas de Concienciación**: Las instituciones financieras podrían llevar a cabo campañas de concienciación para educar al público en general sobre los delitos financieros. Estas campañas podrían incluir anuncios en los medios de comunicación, publicaciones en las redes sociales y eventos comunitarios.

**Formación Continua**: Para los empleados de las instituciones financieras, la formación continua en ciberseguridad y prevención de delitos financieros es esencial. Esto asegura que están al día con las últimas amenazas y las mejores prácticas para prevenirlas.

**Colaboración con Escuelas y Universidades:** Las instituciones financieras podrían colaborar con escuelas y universidades para incorporar la educación sobre delitos financieros y ciberseguridad en sus currículos. Esto ayudaría a educar a la próxima generación sobre estos importantes temas.

También se recomendaría una cooperación internacional ya que como tal la tecnología rompe con cualquier frontera y no cabe duda que las estafas por medios tecnológicos son mayormente cometidos cuando el delincuente se encuentra en otro país por lo cual se recomendaría una asistencia Jurídica Mutua la cual facilitaría la cooperación internacional, también puede facilitar la asistencia jurídica mutua en casos de delitos financieros. Esto puede incluir la extradición de delincuentes, la realización de investigaciones conjuntas y la recuperación de activos robados. Pero para ello se necesitaría facilitar el intercambio de información entre países especialmente en el contexto de los delitos financieros, puede ser un desafío debido a las diferencias en las leyes y regulaciones de privacidad de cada país. Sin embargo, aquí se plantean algunas estrategias que podrían ayudar:

**Acuerdos Bilaterales o Multilaterales**: Los países pueden firmar acuerdos bilaterales o multilaterales que permitan el intercambio de información financiera para la prevención de delitos. Estos acuerdos deben respetar las leyes de privacidad de cada país.

Como ejemplos de estos tipos de acuerdos que se han llevado a cabo tenemos los acuerdos Bilaterales que están Actualmente están en vigor acuerdos de intercambio de información con Andorra, Aruba, Bahamas, Curaçao, San Martín y San Marino. Estos acuerdos permiten el intercambio de información de carácter

tributario entre las administraciones fiscales de los estados (MINISTERIO DE HACIENDA Y FUNCION PUBLICA , 2014).

También podemos encontrar acuerdos con los Estados Unidos el cual este acuerdo se implementó para la mejora del cumplimiento fiscal internacional y la implementación de la Foreign Account Tax Compliance Act - FATCA (Ley de cumplimiento tributario de cuentas extranjeras) (MINISTERIO DE HACIENDA Y FUNCION PUBLICA , 2014).

Desarrollar acuerdos como el de Tax Information Exchange Agreements (TIEA): Los TIEA son acuerdos individuales negociados bilateralmente entre países. A diferencia del CRS, los TIEA son manuales y de uso específico cuando se trata de una evidencia concreta de evasión de impuestos (Librestado, 2018).

“cabe citar la consolidación de los intercambios automáticos entre los Estados Miembros, que permiten que España reciba información sobre distintas categorías de rentas obtenidas en el extranjero por contribuyentes residentes en España.” (Presidencia española consejo de la Union Europea, 2022).

Es importante mencionar que estos acuerdos deben respetar las leyes de privacidad de cada país y se utilizan principalmente para prevenir el fraude y la evasión fiscal (Presidencia española consejo de la Union Europea, 2022).

**Organismos Internacionales**: Organismos internacionales como INTERPOL y Europol facilitan el intercambio de información entre las fuerzas del orden de diferentes países. Estos organismos pueden actuar como intermediarios, asegurando que el intercambio de información se realice de manera segura y legal.

**Redes de Inteligencia Financiera:** Las Redes de Inteligencia Financiera (FINNETs) son organizaciones nacionales que recopilan y analizan información sobre transacciones financieras sospechosas. Estas redes a menudo colaboran entre sí para rastrear el flujo de dinero ilícito a través de las fronteras.

**Normas y Procedimientos Comunes:** Establecer normas y procedimientos comunes para el intercambio de información puede facilitar este proceso. Esto podría incluir normas sobre qué tipo de información se puede compartir, cómo se debe proteger la información y cómo se puede utilizar.

**Tecnología de cifrado**: La tecnología puede desempeñar un papel crucial en el intercambio de información. Las soluciones de cifrado pueden proteger la información durante el intercambio, mientras que las tecnologías de análisis de datos pueden ayudar a las autoridades a identificar patrones y conexiones.

## CONCLUSION

Los resultados de la investigación determinaron una alta conciencia y preocupación entre los encuestados sobre los riesgos de seguridad en línea, especialmente en relación con las transacciones financieras. Sin embargo, hay una percepción generalizada de que las medidas legales y de seguridad actuales pueden no ser suficientes para combatir eficazmente los delitos financieros en línea. Finalmente, la mayoría de los encuestados reconocen que la tecnología, aunque útil, ha aumentado la sofisticación de los delitos financieros.

Los delitos financieros en el entorno digital en Guayaquil, resaltan tres problemas principales. Primero, la libertad para emprender negocios en línea puede conducir a la creación de perfiles no certificados, lo que puede dar lugar a estafas. Segundo, los ciudadanos a menudo confían en los vendedores en línea sin un proceso riguroso de verificación, lo que puede llevar a fraudes. Tercero, algunos couriers confían demasiado en sus clientes y no verifican adecuadamente los pedidos, lo que puede resultar en la circulación de objetos ilegales.

Para mitigar estos problemas, el texto propone dos medidas de seguridad. La primera es la implementación de certificados que aseguren la confianza de los compradores en páginas web, redes sociales y tiendas virtuales. La segunda es

que los couriers implementen un protocolo de seguridad para verificar los pedidos. Estas medidas podrían mejorar la economía del país y la confianza de los ciudadanos en los procesos económicos a través de canales virtuales.

## Bibliografía


Altamirando, L. (29 de 4 de 2020). *REVISTA CHILENA DE DERECHO Y TECNOLOGIA.* Obtenido de El Delito de fraude informatico: Concepto y delimitacion: https://rchdt.uchile.cl/index.php/RCHDT/article/view/57149/61669

Arango, C. (15 de septiembre de 2022). *Qué es el KYC y cómo evoluciona para prevenir delitos financieros*. Obtenido de COBIS TOPAZ: https://blog.cobistopaz.com/es/blog/que-es-kyc-y-como-evoluciona-para-prevenir-delitos-financieros

Asambrea Nacional. (2021). *codigo organico intagral penal.*

Banco Central del Ecuador Subgerencia de Análisis de Productos y Servicios. (2020). *Camarón Ecuatoriano en el Mundo.*

Baracaldo Lozano, N. A., & Daza Giraldo, L. E. (septiembre de 2015). *Panorama de los currículos de programas de contaduria publica en colombia frente a contenidos de auditoria firense y prevencion de delitos financieros.* Obtenido de semanticscholar.org: https://pdfs.semanticscholar.org/81d4/6a689761447f4466370bba9542d31b05c134.pdf?_gl=1*1tdl2id*_ga*OTIyMDcwNTQuMTY5ODE5OTA4NA..*_ga_H7P4ZT52H5*MTY5ODIwNDQxNi4yLjEuMTY5ODIwNDQyNi41MC4wLjA.

Blanco , D. (12 de junio de 2022). *infobae*. Obtenido de www.infobae.com: https://www.infobae.com/economia/2022/06/12/estafas-virtuales-cuales-son-los-delitos-mas-comunes-y-como-prevenirlos/

Caeiro, R. E. (2021). *Documentación de impactos y el método Eslabones de Incidencia. Posibilidades de aplicación INTA.* Buenos Aires: Ediciones INTA; Estación Experimental Agropecuaria Catamarca. Recuperado el 30 de mayo de 2022, de http://hdl.handle.net/20.500.12123/10324

CALDERÓN, V. L. (2020). *LAS NUEVAS PERSPECTIVAS REGULATORIAS DE DELITOS.* RIOBAMBA/ ECUADOR: UNIVERSIDAD NACIONAL DE CHIMBORAZO.

Cámara Nacional de Acuacultura del Ecuador. (17 de 8 de 2022). *Cámara Nacional de Acuacultura*. Obtenido de Reporte de Exportaciones Ecuatorianas Totales: https://www.cna-ecuador.com/estadisticas/

Carrasco, J. B. (2011). *Gestión de procesos (Alineados con la estrategia)*.

Caval , C. (27 de diciembre de 2021). *Abogado.com*. Obtenido de Los tres fraudes más comunes sobre inversiones en la bolsa de valores: https://www.abogado.com/recursos/lesion-personal/fraude-del-corredor-comun/fraude-de-valores-preguntas-frecuentes.html

CFN - Subg. De Análisis de Productos y Servicios. (2020). *EXPLOTACIÓN DE CRIADEROS, PREPARACIÓN Y CONSERVACIÓN, ELABORACIÓN DE PREPARADOS Y VENTAS AL POR MAYOR DE CAMARÓN Y LANGOSTINOS.* GUAYAQUIL.

Chavez Bravo, J., Malpartida Marquez , D., Villacorta Cavero, A., & Orellano Antunez, J. (25 de noviembre de 2020). *La influencia de la automatización inteligente en la detección del cibercrimen.* Obtenido de revista.uta.edu: https://revistas.uta.edu.ec/erevista/index.php/bcoyu/article/view/1462

Cuatrecasas, L. (2017). *Ingeniería de Procesos y de Planta. Ingeniería Lean.* Barcelona: Profit Editorial I. S.L. .

Ecuador, A. N. (15 de marzo de 2022). *codigo civil* . Obtenido de registrocivil.gob.ec: https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2017/05/Codificacion_del_Codigo_Civil.pdf

Editorial etece. (12 de agosto de 2022). *Concepto*. Obtenido de Concepto.de: https://concepto.de/tecnologia/

Enrique, P. L. (2000). *Cejamericas.org.* Obtenido de La seguridad Juridica: una garantia del derecho y la justicia: https://biblioteca.cejamericas.org/bitstream/handle/2015/2606/eserv.pdf

Equipo editorial, E. (5 de agosto de 2021). *Concepto*. Obtenido de Concepto: https://concepto.de/conclusion/

Faes, I. (21 de 02 de 2019). *El Código Penal endurece las penas en los delitos financieros en la línea de las exigencias europeas*. Obtenido de Ecoley: https://www.eleconomista.es/legislacion/noticias/9715151/02/19/El-Codigo-Penal-incorpora-las-exigencias-europeas-y-endurece-las-penas-en-los-delitos-financieros-.html

Fernandez, z. (30 de 8 de 2022). *Significados*. Obtenido de www.significados.com: https://www.significados.com/ciencia

H., B. R. (2004). *Logística. Administración de la cadena de suministro.* . México: Pearson Educación.

Hernandez, R., Baptista, L., & Fernandez , C. (2014). Metodología de la Investigación. En *Metodología de la investigación* (pág. 91). México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

interpol . (2023). *https://www.interpol.int*. Obtenido de INTERPOL: https://www.interpol.int/es/Delitos/Delincuencia-financiera#:~:text=Se%20trata%20de%20actividades%20delictivas,financiera%20nos%20afecta%20a%20todos.

Juarez, C. (5 de julio de 2020). *psicologia y mente*. Obtenido de psicologiaymente.com: https://psicologiaymente.com/reflexiones/frases-john-fitzgerald-kennedy

La Asamblea Nacional . (2014). *CODIGO ORGANICO INTEGRAL PENAL* . LEXIS FINDER.

Librestado. (18 de 10 de 2018). *LIBERTADO* . Obtenido de Cómo funcionan los Acuerdos de Intercambio de Información fiscal (AII o TIEA): https://librestado.com/blog/acuerdos-de-intercambio-de-informacion-aii-tiea/

Lopez Garcia, Y. C. (2021). *Evolución de las finanzas sostenibles en América Latina y el Caribe.* Obtenido de revista diecisiete: https://plataforma2030.org/es/evolucion-de-las-finanzas-sostenibles-en-america-latina-y-el-caribe

Martinez , C. (2018). *Investigación Descriptiva: Tipos y caracteristicas.* Obtenido de Jimcontent.com: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiD6_agw-CAAxVxTjABHZ_xBNAQFnoECCkQAQ&url=https%3A%2F%2Fs9329b2fc3e54355a.jimcontent.com%2Fdownload%2Fversion%2F1545253266%2Fmodule%2F9548087569%2Fname%2FInvestigaci%25C3%25B3n%2520D

MINISTERIO DE HACIENDA Y FUNCION PUBLICA . (29 de 10 de 2014). *Acuerdos de intercambio de informacion*. Obtenido de hacienda.gob.es: https://www.hacienda.gob.es/es-ES/Normativa%20y%20doctrina/Normativa/AcuerdosII/Paginas/acuerdosii.aspx

Palma Alvarado, D. (15 de enero de 2020). *La delincuencia económica en Chile: antecedentes teóricos e históricos sobre los "ladrones de levita y guante", 1880-1920. Historia Mexicana.* Obtenido de semanticscholar.org: https://pdfs.semanticscholar.org/ce47/b6407bf86a2f86d4fcf68a8075552e6ff486.pdf?_gl=1*w78i6y*_ga*OTIyMDcwNTQuMTY5ODE5OTA4NA..*_ga_H7P4ZT52H5*MTY5ODE5OTA4My4xLjAuMTY5ODE5OTA4NS41OC4wLjA.

POLICIA NACIONAL DEL ECUADOR . (2 de 9 de 2015). *POLICIA NACIONAL DEL ECUADOR* . Obtenido de Delitos informáticos o ciberdelitos: https://www.policia.gob.ec/delitos-informaticos-o-ciberdelitos/

Presidencia española consejo de la Union Europea. (27 de 6 de 2022). *Evolución y perspectivas del intercambio de información*. Obtenido de https://sede.agenciatributaria.gob.es/Sede/normativa-criterios-interpretativos/analisis/Evolucion_y_perspectivas_del_intercambio_de_informacion.html

Real Academia Española. (2001). *REAL ACADEMIA ESPAÑOLA*. Obtenido de RAE.ES: https://www.rae.es/drae2001/estafa

Rodriguez, R., Daniel, P. G., & Ana, R. S. (3 de mayo de 2020). *sciencedirectassets.com.* Obtenido de Fraudes financieros, salud y calidad de vida: un estudio cualitativo: https://www.sciencedirect.com/science/article/pii/S0213911119302742

Rubio Rodriguez, G. A., Guido Hernandez, H. A., & Lopez Blandon , A. (febrero de 2021). *ANÁLISIS DE LAS HERRAMIENTAS INFORMÁTICAS UTILIZADAS EN UNA AUDITORÍA FORENSE EN LAS COOPERATIVAS DE AHORRO Y*

*CRÉDITO*. Obtenido de www.revistarefas.com: https://www.revistarefas.com.br/RevFATECZS/article/view/440/304

Servicios, B. C. (2020).

Superintendencia de Compañias Subgerencia de Análisis y Productos y servicios. (2020). *Análisis Sectorial Camarón.*

Toala Indio, Y. (2021). *Delitos informaticos frecuentes en el Ecuador : casos de estudio* . Guayaquil: Universidad POlitecnica Salesiana sede en Guayaquil.

Velasco Melo, A. (2007). *EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001.* Obtenido de www.scielo.org.co: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013

W. Edwards Deming. (1982). *Out of the Crisis. Quality, productivity and Competitive Position.* Ediciones Díaz de Santos, S.A.