UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE COMPUTACIÓN

REVISIÓN DE LITERATURA SOBRE MÉTODOS DE PROTECCIÓN PARA GARANTIZAR CIBERSEGURIDAD EN INSTITUCIONES FINANCIERAS EN EL CONTEXTO ECUATORIANO

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Ciencias de la Computación

AUTOR: ELISEO ISAIAS SALAZAR RODRIGUEZ

TUTOR: JOE LLERENA IZQUIERDO

Guayaquil – Ecuador

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Eliseo Isaías Salazar Rodríguez con documento de identificación N° 0941442865 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 22 de agosto del año 2023

Atentamente,

_____

Eliseo Isaías Salazar Rodríguez

0941442865

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Eliseo Isaías Salazar Rodríguez con documento de identificación No.0941442865, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Revisión de literatura sobre métodos de protección para garantizar ciberseguridad en instituciones financieras en el contexto ecuatoriano", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 22 de agosto del año 2023

Atentamente,

_____

Eliseo Isaías Salazar Rodríguez

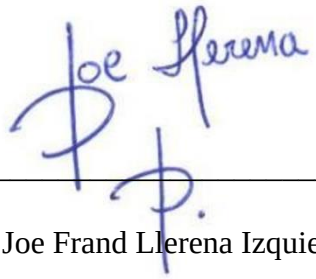
0941442865

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Revisión de literatura sobre métodos de protección para garantizar ciberseguridad en instituciones financieras en el contexto ecuatoriano, realizado por Eliseo Isaías Salazar Rodríguez con documento de identificación N° 0941442865, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 22 de agosto del año 2023

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Este artículo está dedicado con cariño y gratitud a aquellas personas que han sido faros luminosos en mi camino. Sus influencias y apoyo incondicional han sido los cimientos sobre los cuales se erige este trabajo.

A mis padres, cuyo amor, paciencia y sacrificio me han brindado la libertad de perseguir mis sueños y metas. Este logro es un reflejo directo de su inquebrantable confianza en mí.

A mis docentes, quien me ha guiado con sabiduría y paciencia a lo largo de este viaje. Sus enseñanzas y consejos han sido una fuente constante de inspiración y crecimiento.

A mis amigos y colegas, cuya amistad y camaradería han iluminado incluso los momentos más desafiantes. Gracias por ser mi red de apoyo y por celebrar cada pequeño triunfo junto a mí.

A Dios, por ser mi roca, mi confidente y mi mayor fuente de motivación. Tu amor inquebrantable me impulsa a superar mis límites y a esforzarme por alcanzar nuevas alturas.

Esta dedicación es un pequeño reconocimiento de la enorme influencia que cada uno de ustedes ha tenido en mi vida y en la creación de este artículo. Que esta obra sea un testimonio de mi gratitud y aprecio por su presencia constante en mi viaje.

Con cariño,

Eliseo Salazar
Guayaquil, 14 de agosto del año 2023

AGRADECIMIENTO

Quisiera aprovechar esta oportunidad para expresar mi sincero agradecimiento a todas aquellas personas y entidades que contribuyeron de manera significativa en la realización de este artículo. Sus valiosas aportaciones y apoyo incondicional fueron fundamentales para llevar a cabo este trabajo de manera exitosa.

En primer lugar, deseo agradecer a Dios, que es quien siempre ha cuidado de mí y me ha encaminado en el camino correcto, aunque la lucha no fue fácil estoy agradecido porque la cuida de mi en todo tiempo.

También quiero agradecer a mi tutor, Ing. Joe Llerena, cuya orientación experta y sabias sugerencias guiaron cada paso de este artículo. Su compromiso con la excelencia y su disposición a brindar su tiempo y conocimiento fueron inspiradores y motivadores.

No puedo dejar de mencionar el apoyo invaluable proporcionado por mis colegas y amigos, quienes estuvieron dispuestos a debatir conceptos, revisar borradores y brindar aliento en momentos críticos. Sus contribuciones informales y conversaciones enriquecedoras fueron un recordatorio constante de la importancia de un entorno de trabajo colaborativo.

Por último, pero no menos importante, deseo agradecer a mi familia por su inquebrantable apoyo y paciencia a lo largo de este proceso. Sus palabras de aliento y su creencia en mí han sido mi mayor fuente de motivación.

En conjunto, estas contribuciones han desempeñado un papel fundamental en la realización de este artículo. Si bien no es posible mencionar a todos de manera individual, cada uno ha dejado una huella imborrable en este trabajo. Espero que este artículo pueda honrar adecuadamente su generosidad y compromiso.

¡Gracias!
Eliseo Salazar
Guayaquil, 14 de agosto del año 2023

RESUMEN

Últimamente, con el auge de los ataques cibernéticos, las amenazas digitales y el fraude modernos, la seguridad cibernética en las instituciones financieras en Ecuador se ha convertido en un tema crítico. Esta revisión de la literatura examina varios métodos de protección utilizados para garantizar la ciberseguridad en este entorno.

En primer lugar, se destaca la importancia de la formación y sensibilización del personal. Educar sobre prácticas seguras en línea e identificar posibles ataques es fundamental para prevenir violaciones de seguridad. Muchas instituciones financieras ecuatorianas cuentan con programas de capacitación para sus empleados.

A continuación, se analiza el uso de sistemas de autenticación multifactor (MFA). Estos métodos van más allá de las contraseñas tradicionales y requieren una autenticación de varios pasos, como códigos temporales o huellas dactilares. Varios bancos ecuatorianos han introducido MFA para mejorar el acceso a cuentas y datos confidenciales.

Considere también el papel del cifrado de datos. Es imperativo proteger la información confidencial durante la transmisión y el almacenamiento utilizando algoritmos criptográficos sólidos. Las regulaciones ecuatorianas requieren que las instituciones financieras implementen medidas de encriptación para proteger los datos financieros de sus clientes.

Palabras claves: formación, autenticación, encriptación, confidenciales, instituciones.

ABSTRACT

Lately, with the rise of modern cyber-attacks, digital threats and fraud, cyber security in financial institutions in Ecuador has become a critical issue. This literature review examines various protection methods used to ensure cybersecurity in this environment.

First, the importance of training and awareness of staff is highlighted. Educating about safe online practices and identifying potential attacks is critical to preventing security breaches. Many Ecuadorian financial institutions have training programs for their employees.

Next, the use of multi-factor authentication (MFA) systems is discussed. These methods go beyond traditional passwords and require multi-step authentication, such as temporary codes or fingerprints. Several Ecuadorian banks have introduced MFA to improve access to sensitive accounts and data.

Also consider the role of data encryption. It is imperative to protect sensitive information during transmission and storage using strong cryptographic algorithms. Ecuadorian regulations require financial institutions to implement encryption measures to protect their customers' financial data.

Key words: training, authentication, encryption, confidential, institutions.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

La sólida estructura y gobernanza en el país en cuanto a las tecnologías de ciberseguridad tienen como referencia la revisión estratégica y operativa en el Ecuador ya que son esenciales para poder construir un sistema donde los ciberataques no puedan definir ni paralizar la economía o trabajos dentro de instituciones financieras (Aguirre Sánchez, 2021; Coello Ochoa, 2021; Merchan-Lima et al., 2021).

Si bien es cierto esta estrategia contribuye primera estrategia Nacional de ciberseguridad dentro del ecuador, a medida que pasa el tiempo se han venido produciendo nuevos avances loque ha hecho que se tomen medidas proactivas para poder introducir estrategias y obtener mejores resultados (Escalante Quimis, 2021; Zambrano et al., 2019).

Esta revisión de la literatura no solo examina las técnicas de protección empleadas en el contexto ecuatoriano, sino que también aborda las necesidades y los desafíos específicos que enfrentan las instituciones financieras ecuatorianas en su búsqueda continua para fortalecer su ciberseguridad (Catota et al., 2018; Salguero Dorokhin et al., 2019). Hoy en día, se puede decir que la mayoría de las empresas realizan sus actividades financieras de manera más eficiente gracias a las nuevas tecnologías (Reyes-Mena et al., 2018). La tecnología es una herramienta fundamental para que las organizaciones sean más productivas, cubran más mercados y creen nuevos canales de comunicación con clientes y proveedores (Rea-Guaman et al., 2020). Sin embargo, este nuevo entorno requiere que las empresas se adapten al nuevo sistema operativo y proporcionen seguridad de datos de alta calidad a sus sistemas para que puedan evitar ataques (Catota et al., 2019).

En la actualidad las instituciones financieras a nivel mundial viven una desconexión como comunidad, ya que las autoridades financieras se enfrentan a riesgos específicos de ciberamenazas, que siguen siendo poco eficaz a la hora de participar y poder afrontar las amenazas, según la cooperación en cuestiones de ciberseguridad se ha visto un poco fragmentada, así como reducido los círculos de confianza ya que atañe los intereses de la seguridad nacional (Quezada-Sarmiento et al., 2023; Terán Villafuerte, 2023)

En el entorno que se encuentran las instituciones a nivel de América Latina las ciber amenazas y riesgos son provenientes de ciberespacios los cuales son un reto al momento de salvaguardar la seguridad, en este sentido las primeras acciones que se han tomado es comprender el nivel

de riesgos y amenazas actuales para poder consolidar la fase inicial y desarrollar un sistema de ciberseguridad a un nivel más alto (Carballo & Villagran Gómez, 2023; Terán Villafuerte, 2023)

El enfoque que ha tenido la ciberseguridad en las instituciones financieras a nivel nacional se encontró que el 50% de las empresas, han implementado un programa de concientización en ciberseguridad para empleados, empleamos la frase "el eslabón más débil de las instituciones son los empleados", sin embargo en un 70% las instituciones afirman de que no tiene la efectividad del proceso de respuesta antes estos incidentes de ciberseguridad, teniendo en cuenta estas cantidades, una de las cosas que detienen a muchas de las instituciones es el presupuesto implementado hacia la ciberseguridad, que es lo que detiene a la implementación (Terán Villafuerte, 2023)

2. REVISIÓN DE LITERATURA

Según (Terán Villafuerte, 2023), la situación en los sistemas de ciberseguridad en las instituciones financieras se base en diseñar, implementar y mantener estrategias de ciberseguridad efectivas. La combinación adecuada de estos conceptos puede ayudar a reducir el riesgo de amenazas cibernéticas y mitigar los impactos potenciales a nivel mundial. Por ejemplo, el principio de menor privilegio, este principio establece que los usuarios y procesos deben tener solo los permisos necesarios para realizar sus funciones. Limitar el acceso innecesario ayuda a minimizar el impacto de amenazas internas y externas (Carballo & Villagran Gómez, 2023).

La defensa en profundidad definida como un enfoque que se basa en la idea de que la seguridad no debe depender de una única medida de protección. En cambio, se implementan múltiples capas de seguridad para reducir la exposición a amenazas (Quezada-Sarmiento et al., 2023). La autenticación verifica la identidad de los usuarios y la autorización controla qué acciones pueden realizar. Estos conceptos garantizan que solo los usuarios legítimos tengan acceso a los recursos adecuados (Sánchez Peña & others, 2023).

La encriptación convierte los datos en un formato ilegible para cualquier persona no autorizada. Esto ayuda a proteger la confidencialidad de la información, incluso si se intercepta (Diaz Jimenez et al., 2023; Sánchez Peña & others, 2023). Dividir las redes en segmentos aísla los sistemas críticos y limita la propagación de amenazas. Incluso si un segmento se ve

comprometido, el daño puede mantenerse bajo control (Nieto Rodríguez & Sánchez Rojas, 2023).

Establecer políticas y procedimientos claros para el uso de sistemas y datos ayuda a mantener una postura de seguridad coherente en toda la organización (Sánchez Castillo & others, 2023). Monitorear el comportamiento del usuario y del sistema puede revelar actividades anómalas o maliciosas que no se detectarían mediante análisis estáticos. Mantener el software y los sistemas actualizados con las últimas correcciones de seguridad ayuda a cerrar las vulnerabilidades conocidas. La supervisión constante de eventos y registros permite identificar actividades inusuales y proporciona una visión detallada de lo que está ocurriendo en los sistemas (Urgell et al., 2023).

La formación de los empleados y usuarios sobre las amenazas cibernéticas y las mejores prácticas de seguridad es esencial para crear una cultura de ciberseguridad. Evaluar y priorizar los riesgos de seguridad cibernética ayuda a tomar decisiones informadas sobre las medidas de protección que deben implementarse (Quezada-Sarmiento et al., 2023). Tener un plan de respuesta a incidentes establece procesos claros para abordar rápidamente las amenazas cuando se produzcan. La colaboración con otras organizaciones y la participación en redes de intercambio de inteligencia de amenazas ayudan a mantenerse informado sobre las últimas tácticas y amenazas (Cabrera & Galarza, 2022).

En el trabajo de análisis (Terán Villafuerte, 2023). Se requiere establecer procedimientos con métodos efectivos para guardar la integridad y fiabilidad de la información de procesos internos, como lo son los aplicativos de la institución, así también como políticas internas, manuales, etc.

Por eso cada los sistemas de control y accesos lógicos internos de la institución son importantes para garantizar una institución con ciberseguridad, ya que el robo, fraude o extracto de información sensible obstaculizaría los objetivos del negocio (Quezada-Sarmiento et al., 2023).

Las instituciones financieras suelen ser el objetivo de los ataques cibernéticos porque manejan información confidencial, como información financiera y personal de los clientes (Tacuri López, 2021)(Recalde Monar, 2021)(Terán Villafuerte, 2023). Dada la naturaleza específica de Ecuador y los cambios constantes en tecnología y amenazas cibernéticas, es importante consultar fuentes actualizadas y específicas de Ecuador para obtener información detallada sobre cómo las instituciones financieras en esta provincia enfrentan la seguridad cibernética

(Mayorga Muñoz, 2022; Melendrez-Caicedo & Llerena-Izquierdo, 2022; M. A. Reyes Sarmiento, 2022)

Los delitos informáticos han traído perjuicios económicos, razón por la cual la CEPAL (Comisión Económica para América Latina y el Caribe) declaró que, en América Latina, el 45,5% de los hogares tiene ataque a Internet, de aquellos hogares con conexiones maduras, como Costa Rica, Uruguay y Chile, más del 56%; mientras que en Ecuador, Perú, Colombia, Venezuela y México varía entre 15 y 45 por ciento (Analytica, 2018; Demertzi et al., 2023; Ozdemir et al., 2022; Tsymbal et al., 2023) De esta forma, los ecuatorianos en el balance de los delitos informáticos se ven privados de buenos conocimientos tecnológicos para albergar una inteligente y mejor previsión tecnológica en el país, seguros de que se van a hacer cargo de posibles bancas electrónicas, generalmente gente sin escrúpulos, maliciosos y con amplios conocimientos en tecnologías de la información realizan prácticas que violan impuestos ajenos por el clima de Internet (Pérez González, 2021; Riggs et al., 2023; Toala Indio, 2021).

2.1. CIBERATAQUES CONTRA INSTITUCIONES FINANCIERAS

Algunas de las instituciones financieras encuestadas son intermediarios del mercado de valores y se sabe que son altamente productivas, asimismo bancos de ahorro o préstamo, o instituciones interoperables de depósito e inversión (Kang, 2023; K. T. Smith et al., 2023). Como parte de la definición de un ciberataque, el Observatorio Económico y Productivo de la ESPOCH, con sede en la ciudad de Morona y Santiago, realizó un estudio de los avances tecnológicos, incluyendo el uso cotidiano de herramientas digitales, además contiene algunas historias desarrolladas de ataques contra instituciones financieras (Adelmann et al., 2020; Herrera Luque et al., 2021; Lee & Lee, 2023; Molina Castaño, 2021; Ramírez et al., 2017).

Se puede comprobar la naturaleza del riesgo para detectar el riesgo de fraude informático, que representa una de las principales amenazas o vulnerabilidades, así lo afirman varios autores (García Wirton, 2021; Kalogiannidis et al., 2023) Para estos autores, el fraude es uno de los delitos informáticos más comunes, presentando vulnerabilidades y amenazas constantes. Estos grupos criminales están fuertemente protegidos y han evolucionado a nivel nacional e internacional utilizando las últimas tecnologías para atacar redes de instituciones financieras (Chen et al., 2023).

2.2. EL ENTORNO DE LA CIBER-RESILIENCIA

La ciber resiliencia se ha convertido recientemente en uno de los conceptos más publicitados en las discusiones sobre ciberseguridad (Linkov & Kott, 2019), a pesar de, o quizás debido a, su significado nebuloso, lo que dificulta su definición y medición rigurosa (Dupont, 2019)(Hausken, 2020). Su popularidad está indudablemente ligada a los numerosos titulares sobre ciberataques y filtraciones de datos que salpican las portadas de periódicos y sitios web de tecnología, anunciando información sobre hackers nuevos y masivos que revelan la fragilidad de nuestras infraestructuras digitales y la incapacidad de las organizaciones para proteger los datos personales que encomendarles (Linkov et al., 2023; S. Smith, 2023). Incluso las organizaciones más conocedoras de la tecnología y conscientes de la seguridad no son inmunes a las fallas catastróficas de ciberseguridad (Pavão et al., 2023). Una vez que aceptan el hecho de que operan en un estado permanente de vulnerabilidad cibernética mientras obtienen considerables beneficios de productividad de las tecnologías que también amenazan su existencia, deben aprender a *"sobrevivir con una dieta de fruta envenenada"* (Bagheri et al., 2023; Noel et al., 2023).

En palabras de uno de los padres fundadores del concepto este cambio de perspectiva *"no requiere una capacidad precisa para predecir el futuro, sino solo una capacidad cualitativa para diseñar sistemas que puedan absorber y acomodar eventos futuros en cualquier forma inesperada que puedan tomar"* (Dupont, 2019; Garcia-Perez et al., 2023). Aunque la resiliencia y la gestión de riesgos están relacionadas, es importante distinguir entre las dos (Chen et al., 2023). La gestión de riesgos es la cuantificación de la probabilidad y la gravedad del riesgo para que pueda respaldar las decisiones sobre las estrategias más adecuadas para gestionar el riesgo, tales como la omisión, elusión, reducción, transferencia y aseguramiento (Demertzi et al., 2023; Herrera Luque et al., 2021). La resiliencia tiene un alcance más amplio y es *"esencial cuando los riesgos son mutuamente excluyentes, por ejemplo, cuando surgen repentinamente situaciones peligrosas o cuando los paradigmas de análisis de riesgos resultan ineficaces"* (Karimi et al., 2023; Kelli et al., 2021).

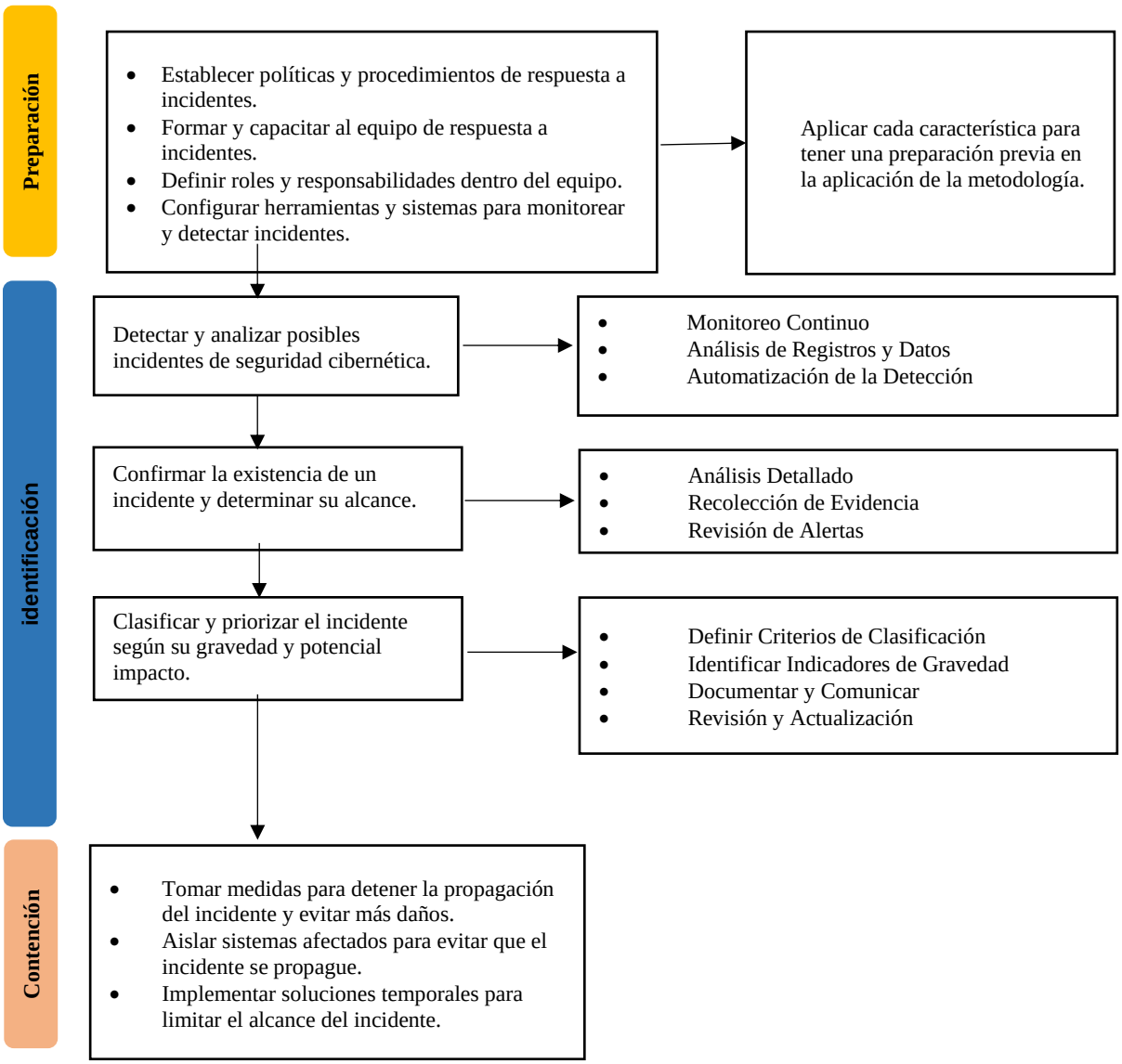
3. METODOLOGÍA

En el estudio y análisis realizado, propone una metodología de investigación descriptiva, de corte cuantitativo. Analiza en profundidad los métodos de protección para garantizar la ciberseguridad frente a la medición de fraudes cibernéticos durante los últimos años mediante

una revisión de literatura, de este modo la información permite medir el nivel, el impacto y la adaptabilidad que han tenido las instituciones financieras en base a criterios en ciberseguridad, de esta manera describir las fases y preguntas de investigación en relación con los ataques cibernéticos como también las vulnerabilidades del sistema financiero.

En la metodología de trabajo implementada se determinan acciones que involucren procesos en los métodos de protección de sistemas, redes, datos y activos digitales de amenazas y ataques cibernéticos.

Figura 1. Procesos de métodos de protección



Para esto se plantearon las preguntas de investigación, (ver Tabla 1).

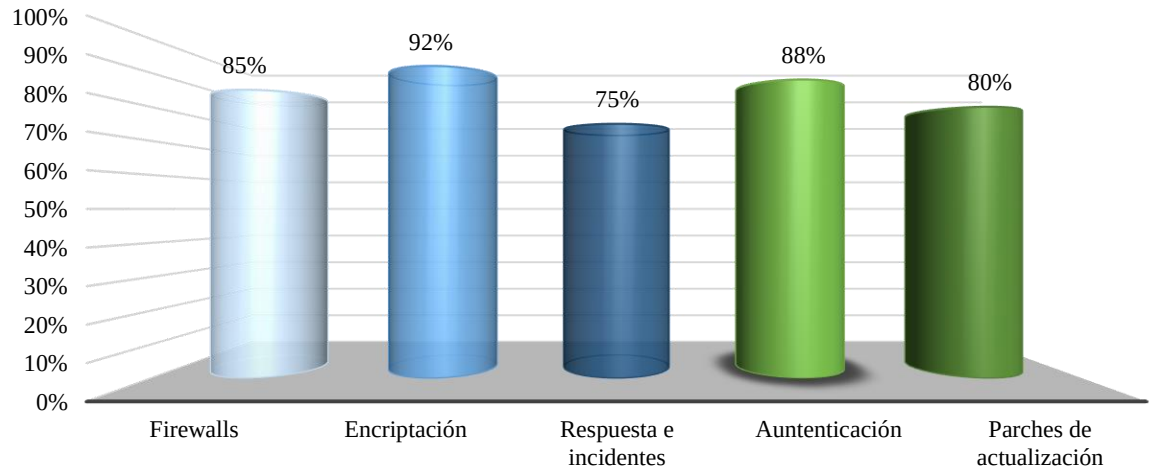
Tabla 1.Preguntas de investigación y análisis.

¿Cuáles son los métodos de protección cibernética más comúnmente utilizados en instituciones financieras ecuatorianas?
¿Cuál es el nivel de adopción de tecnologías de autenticación y cifrado en las instituciones financieras en Ecuador?
¿Cuál es el impacto de los ataques cibernéticos en la confianza de los clientes en las instituciones financieras ecuatorianas?
¿Cómo ha evolucionado la regulación y legislación en ciberseguridad para instituciones financieras en Ecuador?

Los métodos de protección para determinar el nivel de incidencias que existen dentro de las instituciones ecuatorianas se desarrollan a través de procesos lo cuales sirven para fortalecer la infraestructura ya que se debe encontrar donde se encuentra la parte más crítica, ya sea por medio de monitoreo de incidencias a través de informes, las auditorias y análisis dentro de la institución para encontrar las vulnerabilidades físicas y lógicas (Nieto Rodríguez & Sánchez Rojas, 2023; Sánchez Peña & others, 2023; Urgell et al., 2023).

Nos referimos a infraestructura critica cuando hablamos de las instalaciones, redes, sistemas y equipos físicos y de tecnología de información las cuales se encuentra el funcionamiento de los servicios de la institución, (ver Fig. 2).

Figura 2. Promedio de efectividad de protección



Podemos determinar los incidentes mediante métodos de protección los cuales en la (Fig. 2), se encuentra detallado el porcentaje y nivel de efectividad que tienen como métodos de protección.

- Firewalls: Se la utiliza como primera línea de defensa a nivel de redes.

- Encriptación: Es esencial para la protección de datos sensibles.
- Respuesta a Incidentes: Se tiene un control rápido del detalle de incidentes.
- Autenticación Multifactor: Aumenta el nivel de seguridad en plataformas y aplicativos.
- Actualización de Software: Los parches a los equipos cierran vulnerabilidades

Con el pasar de los años con las auditorías internas y externas, las observaciones que han tenido con las instituciones financieras y como beneficios de último momento en el ámbito ecuatoriano se aprobó la norma de protección de datos lo que ha hecho que muchas instituciones mejores sus sistemas de seguridad por obligación a que los derechos de las personas deben ser confidencialmente guardadas de acorde a las normas, asimismo las certificaciones en algunas de las instituciones hacen que se guarde la integridad de las personas (clientes) (Alawida et al., 2022)(Rameem Zahra et al., 2022), implementando las metodologías hacen que el número de ataques y accesos disponibles para cualquier colaborador sean menores, también como el control de accesos y la implementación de múltiples herramientas como lo son los códigos OTP (Park et al., 2023)(Aparicio et al., 2023), los métodos de autenticidad hacen disminuya estos ataques hacia los clientes, como podemos visualizar en la ilustración, (ver Fig. 3).

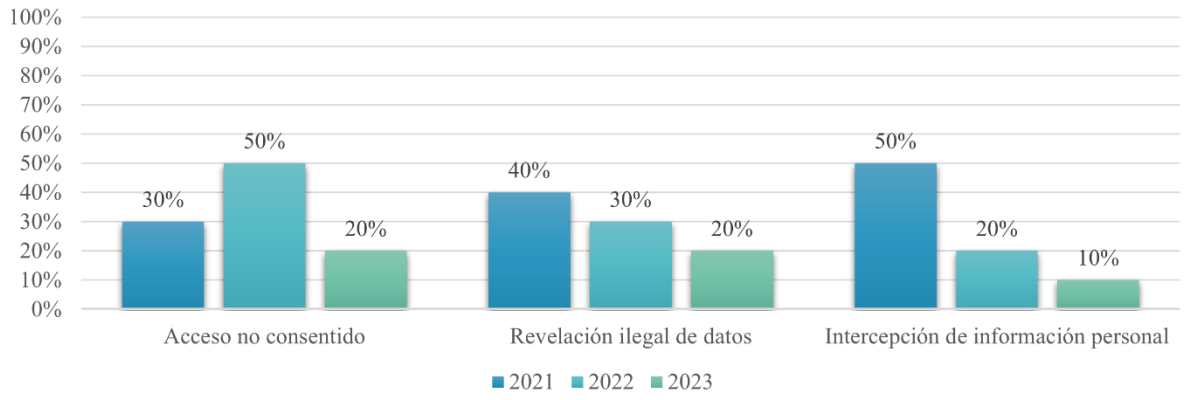


Figura 3. Estadística en la implementación de metodologías para reducir el nivel de ciber-ataques.

Esto ha permitido que las personas se sientan más seguras ya que las instituciones dan la confianza para poder guardar su dinero en cuentas de las instituciones, así también como depositar información de créditos, con la seguridad y certificaciones que tengan las empresas ayuda mucho al negocio, ya que los clientes acogen el concepto de sentirse seguros.

En la revisión realizada se dio alcance las siguientes preguntas las cuales cada una tiene un concepto distinto en el ámbito de la ciberseguridad entre ellas revisamos lo factible de los métodos implementados en cada una de ellas.

- Amenazas Cibernéticas Comunes
- Impacto de Ataques
- Métodos de Protección Tradicionales
- Tecnologías Emergentes

4. RESULTADOS

¿Cuáles son los métodos de protección cibernética más comúnmente utilizados en instituciones financieras ecuatorianas?

El método para garantizar la ciberseguridad es un proceso que implica la aplicación planificada y organizada de medidas y controles de seguridad para proteger los sistemas, datos y recursos de una organización de posibles amenazas cibernéticas. Lo que se propone en el método es realizar evaluaciones las cuales se lleven a cabo diferentes propuestas ya que siempre existirá un margen de error, eso es lo que se busca en cuanto a instituciones mitigar ese margen de error, para que los clientes de dicha institución tengan la seguridad y confianza de que todos sus datos personales están guardados en una base de alta seguridad al igual que sus ingresos o transferencias, asimismo el establecimiento de objetivos e implementación de nuevos sistemas estos sean menos complejos al momentos de ejecutarse, los procesos que existen en una institución deben ser integrados para cualquier tipo de servicio ya que siempre hay actualizaciones (Alcívar-Cruz & Llerena-Izquierdo, 2023; Urgell et al., 2023), eso quiere decir que el método que se implemente debe realizarse de manera continua para llevar a cabo una integración entre las demás instituciones.

La economía de las API permite la transformación de una empresa u organización en una plataforma. Las plataformas multiplican la creación de valor al permitir el consumo de coincidencias entre usuarios dentro y fuera de los ecosistemas empresariales y facilitando la creación y/o el intercambio de bienes y servicios con el uso de tecnologías como la inteligencia artificial (Sánchez Castillo & others, 2023; Sanchez-Romero & Llerena-Izquierdo, 2023), y acciones sociales para que todos los participantes puedan aportar valor (Cabrera & Galarza, 2022; Zerega-Prado & Llerena-Izquierdo, 2022).

Sistemas de banca web incorpora un tipo de arquitectura abierta orientada a servicios (SOA) que permite una mayor flexibilidad técnica y comercial, facilitando la escalabilidad, integración y coexistencia con otras aplicaciones (Malinka et al., 2022). SOA es un método que se puede utilizar para lograr tiempos de respuesta óptimos en los procesos y así adaptarse rápidamente a las necesidades del mercado (Díaz Redondo et al., 2021). Durante algún tiempo, los activos digitales se han vuelto cada vez más valiosos, el entorno geopolítico se ha endurecido y las expectativas de los clientes y los reguladores se han vuelto cada vez más estrictas (Karim & Hasan, 2021).

Las empresas de servicios financieros deben desarrollar una estrategia organizacional para construir una sólida postura de seguridad cibernética en este entorno disruptivo (Mytnyk et al., 2023). No hay duda de que la ciberseguridad es un problema comercial que requiere un esfuerzo de toda la empresa, para que se pueda llevar a cabo necesitados procesos los cuales ayudaran a que la metodología se pueda implementar (Haruna et al., 2022), (ver Fig. 4).

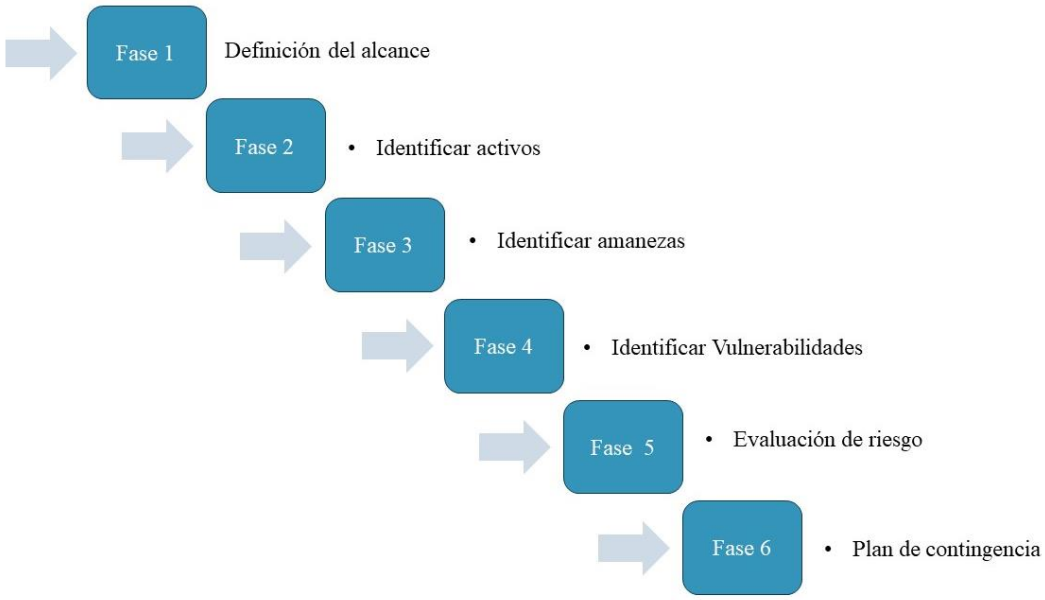


Figura 4. Proceso de método para garantizar ciberseguridad

Definición del alcance

El alcance en ciberseguridad se refiere a la delimitación precisa y específica de los sistemas, activos, procesos y áreas que serán objeto de análisis, protección, monitoreo y evaluación en el contexto de las medidas de seguridad cibernética. Definir el alcance es esencial para establecer

límites claros y garantizar que los esfuerzos de seguridad estén dirigidos de manera efectiva y eficiente hacia los recursos y riesgos relevantes.

Identificar activos

En el ámbito de la ciberseguridad, un activo se refiere a cualquier recurso o componente que tenga valor para una organización y que requiera protección contra amenazas y riesgos cibernéticos. Identificar y clasificar correctamente los activos es un paso fundamental para desarrollar estrategias efectivas de ciberseguridad.

Identificar amenazas

Las amenazas en ciberseguridad son posibles eventos o situaciones que tienen el potencial de causar daño, interrupción o compromiso en los activos de una organización. Identificar estas amenazas es fundamental para implementar medidas de seguridad adecuadas y mitigar los riesgos.

Identificar Vulnerabilidades

Las vulnerabilidades en ciberseguridad son debilidades o puntos débiles en sistemas, aplicaciones, redes o procesos que pueden ser explotados por amenazas para comprometer la seguridad y causar daño. Identificar vulnerabilidades es crucial para tomar medidas preventivas y correctivas para proteger los activos de una organización.

Evaluación de riesgo

La evaluación de riesgos en ciberseguridad es un proceso fundamental para identificar, analizar y priorizar las posibles amenazas y vulnerabilidades que podrían afectar a una organización. Su objetivo principal es comprender los riesgos cibernéticos a los que está expuesta la organización y tomar decisiones informadas para mitigarlos.

Plan de contingencia

El plan de contingencia en ciberseguridad es un conjunto de medidas y procedimientos predefinidos que una organización sigue para responder de manera efectiva a incidentes de seguridad cibernética y minimizar el impacto en caso de que ocurran.

¿Cuál es el nivel de adopción de tecnologías de autenticación y cifrado en las instituciones financieras en Ecuador?

Ofrecer a los clientes y/o usuarios los mecanismos necesarios para ello personalizar las condiciones en las que desean realizar sus transacciones a través de canales y diferentes tarjetas electrónicas, en ellos condiciones o límites máximos que deben fijarse y deben ser propiedad de cada entidad validar o verificar la autenticidad de los clientes a través de métodos de autenticación, esto sirve de alguna manera para que el nivel de tecnologías aumente así como su seguridad dentro de cada institución (M. A. Reyes Sarmiento, 2022).

Dentro de las instituciones financieras se manejan varios sistemas los cuales conforme se van mejorando los mismos, se deben implementar nuevos niveles de seguridad para tener una adaptación de las tecnologías.

A continuación se presenta en la tabla 2, aquellas adaptaciones tecnológicas existentes de Ciberseguridad de acuerdo con los niveles de adaptación en la organización, siendo el nivel 0 como no implementado, nivel 1 como exploratorio (en estudio por la organización), el nivel 2 como implementado, nivel 3 como avanzado y nivel 4 como optimizado, (ver Tabla 2).

Tabla 2. Tabla de niveles de adopción

Tecnología de Ciberseguridad	Nivel 0 (No implementado)	Nivel 1 (Exploratorio)	Nivel 2 (Implementado)	Nivel 3 (Avanzado)	Nivel 4 (Optimizado)
Firewalls	No se han implementado firewalls.	Firewalls se están evaluando, pero no se han implementado completamente.	Firewalls básicos se han implementado, pero la configuración puede ser inconsistente.	Firewalls avanzados y configurados de manera consistente para todas las redes.	Firewalls avanzados con análisis constante y ajuste para maximizar la seguridad.
Antivirus	No se han implementado soluciones antivirus.	Se están explorando diferentes soluciones antivirus.	Soluciones antivirus básicas se han implementado, pero no están integradas en todos los sistemas.	Soluciones antivirus implementadas en todos los sistemas y se actualizan regularmente.	Soluciones antivirus avanzadas con análisis heurístico y protección en tiempo real.
Detección de Intrusiones	No se han implementado sistemas de detección de intrusiones.	Se está considerando la implementación de sistemas de detección de intrusiones.	Sistemas de detección de intrusiones básicos se han implementado, pero las alertas pueden ser ignoradas.	Sistemas de detección de intrusiones activos y gestionados, y se realizan investigaciones sobre alertas.	Sistemas de detección de intrusiones avanzados con análisis de comportamiento y respuesta automatizada.
Gestión de Identidad	No se ha implementado una solución de gestión de identidad.	Se están investigando soluciones de gestión de identidad.	Solución básica de gestión de identidad implementada, pero la autenticación puede ser débil.	Solución de gestión de identidad robusta implementada con autenticación multifactorial.	Solución de gestión de identidad avanzada que abarca la autenticación, autorización y control de acceso.

Encriptación	No se ha implementado encriptación de datos.	Se están evaluando opciones de encriptación de datos.	Encriptación básica de datos se ha implementado en algunos sistemas.	Encriptación de datos implementada en todos los sistemas críticos y comunicaciones.	Encriptación avanzada con claves seguras y políticas de gestión de claves.

Fuente: Elaboración Propia

¿Cuál es el impacto de los ataques cibernéticos en la confianza de los clientes en las instituciones financieras ecuatorianas?

El incremento de los canales digitales y la adaptación de los modelos de negocio bancario a la digitalización va acompañado de fuertes esquemas de seguridad para reducir diversos tipos de ciberataques al sector y, por supuesto, a sus clientes. Es el sector de la banca privada el que es uno de los más regulados y controlados del país, y en esta situación siempre actúa de acuerdo con todas las normas de ciberseguridad pertinentes, y además cumple con los más altos estándares aplicados por la industria (T. P. Reyes Sarmiento, 2022), (ver Tabla 3).

Tabla 3. Tabla de impacto

Tipo de Ataque	Impactos	Niveles de impacto en el contexto ecuatoriano
Malware y Ransomware	Pérdida de datos, interrupción de operaciones, pérdida financiera por rescate, daño a la reputación.	MEDIO
Ataques de Denegación de Servicio (DDoS)	Interrupción de servicios en línea, pérdida de ingresos, daño a la reputación.	BAJO
Phishing y Ingeniería Social	Robo de credenciales, acceso no autorizado a cuentas, pérdida financiera, robo de identidad.	ALTO
Ataques de Inyección	Exposición de datos sensibles, manipulación de sistemas, acceso no autorizado.	BAJO
Ataques de Ingeniería Inversa	Robo de propiedad intelectual, exposición de código fuente, pérdida de ventaja competitiva.	MEDIO
Fugas de Datos	Pérdida de confianza de los clientes, daño a la reputación, posibles sanciones legales.	MEDIO
Acceso no Autorizado	Fugas de datos, exposición de información sensible, pérdida de confianza.	MEDIO
Riesgos a la Privacidad	Violaciones de regulaciones de privacidad, pérdida de confianza de los clientes.	ALTO

Fuente: Elaboración Propia

El impacto que ha tenido cada uno de los diferentes ataques descritos, en la tabla se definen como alto, medio y bajo, que es el impacto que ha tenido dentro de las instituciones financieras a nivel nacional.

¿Cómo ha evolucionado la regulación y legislación en ciberseguridad para instituciones financieras en Ecuador?

Las firmas financieras son responsables de administrar los riesgos que enfrentan cuando subcontratan servicios a terceros, particularmente aquellos que respaldan procesos críticos.
En Ecuador se señalan algunas medidas implementadas por el gobierno central, como el Comité Nacional de Ciberseguridad, que está integrado por representantes de diversas instituciones. Actualmente, el país recibe apoyo de organismos internacionales como la Unión Europea (Cyber4Dev), el Banco Mundial y otros organismos internacionales (García Wirton, 2021). Se puede entender que la evolución de los métodos de protección en ciberseguridad se ha ido realizando debido a los incidentes en el tiempo, (ver Fig. 4).

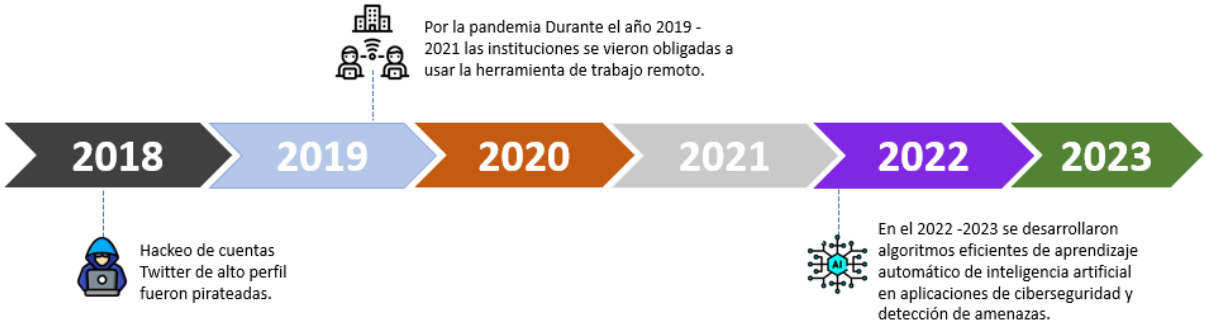


Figura 4. Evolución de la ciberseguridad en el tiempo

4.1. ANALISIS DE RESULTADOS

En los últimos tres años se ha demostrado que haber separado el área de ciberseguridad a un área aislada, ha hecho que se pueda realizar distintos procesos para levantar la calidad y seguridad en la banca ecuatoriana, lo que ha dejado mucho de qué pesar ya que los ataques cibernéticos en transacciones tanto nacional o a nivel internacional han subido. Aunque sea un país poco capacitado a nivel de ciberseguridad, no somos los únicos países en Latinoamérica, el cual reciben ataques, tanto empresas como instituciones financieras, los más grandes hackers se actualizan constantemente, incluso con la llegada y actualizada inteligencia artificial que está teniendo un rol importantísimo a niveles extremos en los últimos tiempos, por lo que esto ha llevado a que la industria bancaria sea líder en implementación de cambios en servicios tecnológicos, claro está que muchas veces el presupuesto para las instituciones deben acoplarse, porque existen normas que lo exigen para que no haya fraudes transaccionales, fraudes de suplantación, etc.

4.2. ANÁLISIS DE LAS NECESIDADES Y DESAFÍOS

A medida que ha avanzado la tecnología se encuentran varias razones por la cuales ha n hecho que se lleve a cabo el desarrollo de nuevas tecnologías, de nuevos sistemas los cuales desde años atrás según, (Garcia Wirton, 2023) se dieron a conocer de manera fuerte, como lo fue con las tecnologías de conexión remota, a que empezó el tiempo de pandemia, esto creo la necesidad de implementar dicha conexión, claro que esto ha hecho que han más ciberataques por parte de colaboradores de la institución.

Las nuevas herramientas de trabajo como las videoconferencias, las soluciones en la nube, servicios y tecnologías de acceso remoto, herramientas colaborativas,, estas mismas han causado que hayan más brechas para los atacantes a que desde un punto de vista no se puede monitorear cada paso que den los colaboradores a que se conectan desde cualquier red doméstica, así mismo los del área responsable se han visto e la obligación de agregar nuevas políticas para la implementación de dichas herramientas, (ver Tabla 4).

Tabla 4. Necesidades y Desafíos ante ciberataques.

Necesidades	Desafíos
Protección de Datos Sensibles	Evolución de Amenazas
Continuidad de Operaciones	Ataques Dirigidos
Cumplimiento Regulatorio	Personalización de Ataques
Prevención de Fraude	Cumplimiento Complejo
Gestión de Riesgos	Gestión de Identidades
Capacitación del Personal	Amenazas Internas

Las instituciones financieras enfrentan una serie de necesidades y desafíos en términos de ciberseguridad. Proteger los datos, garantizar la continuidad de las operaciones, cumplir con regulaciones, prevenir el fraude y gestionar riesgos son fundamentales en un entorno donde las amenazas cibernéticas son cada vez más complejas y frecuentes. La colaboración entre expertos en ciberseguridad, la inversión en tecnologías adecuadas y la educación continua del personal son elementos esenciales para abordar estos desafíos de manera efectiva.

Estos ataques pueden tener consecuencias graves para la seguridad de los datos, la confianza del cliente y la estabilidad económica. Algunas de las afectaciones y tipos de ataques más comunes incluyen:

- Robo de Datos y Fraude Financiero
- Ataques de Denegación de Servicio (DDoS)

- Ransomware
- Phishing e Ingeniería Social
- Malware y Espionaje Cibernético
- Fuga de Datos y Violación de la Privacidad
- Falta de Disponibilidad
- Impacto en la Confianza

Como medida de prevención es importante que las instituciones financieras implementen medidas sólidas de seguridad cibernética, como firewalls, autenticación multifactor, gestión de vulnerabilidades y planes de respuesta a incidentes, para mitigar estas amenazas.

En la siguiente tabla se muestran el impacto que ha tenido la ciberseguridad en cuanto ataques a las instituciones financieras:

Tabla 5. Afectaciones más importantes suscitadas.

Año	Número de incidentes	Descripción del ataque	Consecuencias	Método de protección	Referencias
2021	10	Ataques de phishing a empleados, intentos de acceso no autorizado a sistemas bancarios	Pérdida de datos confidenciales, intentos de fraude financiero	Mejora de la formación en seguridad para empleados, fortalecimiento de medidas de autenticación	(Kaur et al., 2021) (Humayun et al., 2021) (Kim et al., 2021) (Miller et al., 2021) (Wade, 2021) (Mat et al., 2021) (Karim & Hasan, 2021) (Nawa et al., 2021) (Amarullah et al., 2021) (Ife et al., 2021)
2022	8	Ransomware dirigido a instituciones financieras, interrupción de servicios en línea	Paralización de operaciones, demandas de rescate	Restauración de sistemas a partir de copias de seguridad, cooperación con fuerzas de seguridad	(Tsai et al., 2022) (Kaoudi & Quiané-Ruiz, 2022) (Ahmad et al., 2022) (Ouafiq et al., 2022) (Nambiar & Mundra, 2022) (McDonald et al., 2022) (Rameem Zahra et al., 2022) (Islam et al., 2022)
2023	12	Fugas de datos de tarjetas de crédito, explotación de vulnerabilidades en aplicaciones móviles	Robo de información financiera, fraude en tarjetas	Parches de seguridad para las aplicaciones, notificación a los clientes afectados	(Ao, 2023) (Winker et al., 2023) (Gümüşboğa & Duruk, 2023) (Lehmann et al., 2023) (Yamini et al., 2023) (Mytnyk et al., 2023) (Aftabi et al., 2023) (Velicheti et al., 2023)

					(Aftabi et al., 2023) (Lakshmi et al., 2023) (Dasgupta et al., 2023) (Gulyás & Kiss, 2023)

Fuente: Elaboración propia.

5. DISCUSIÓN

El tema escogido en los "Métodos de Protección para Garantizar Ciberseguridad en Instituciones Financieras en el Contexto Ecuatoriano" es altamente relevante en el mundo actual, donde las amenazas cibernéticas están en constante evolución. Las instituciones financieras son particularmente sensibles a tales amenazas debido a la naturaleza confidencial y valiosa de los datos que manejan.

En el sistema actual donde las tecnologías de información y protección de datos son altamente de riesgo alto ya que cada vez aumentan las vulnerabilidades debido al hecho de la inteligencia artificial (IA), debido a que cada vez está más de moda donde los la creación de virus, troyano, ransomeware que son cada vez más feroces, ya que tenemos al cuidado de los servicios cibernéticos es un tema que se menciona ampliamente debido a las formas de espionaje cibernético, por esta razón, varios países del mundo han adoptado estrategias para proteger sus sistemas, evitando las situaciones adversas de los mismos, en Ecuador, un menor el sistema de defensa cibernética se puede apreciar en comparación con los países desarrollados.

Claro está que el tema contractual es un importante trayecto que se puede decir que con el pasar de los años se ha ido avanzando, lo que el articulo proporciona y contempla es la garantía de poder proporcionar una protección a nivel de ciberseguridad en las instituciones financieras, contemplar el hecho de que existen métodos a implementar, así como herramientas las cuales sirven para dar cabida que no haya los fraudes bancarios.

Haciendo énfasis en que empezar por un cambio dentro de nuestro país se puede desarrollar conocimientos y capacidad en ciberseguridad para estar mejor representados en discusiones que afectan a nuestros ciudadanos y organizaciones, y ser un socio confiable y contribuyente a nivel regional y global.

6. CONCLUSIÓN

En la investigación hemos demostrado como se enfrentan a series de amenazas y vulnerabilidades en las instituciones financieras debido a que la naturaleza de los datos y servicios financieros que manejan.

He identificado que se ha podido medir el nivel de incidencias a nivel de instituciones financieras, plantear políticas de seguridad la cual por medio de procesos y metodologías que pueden ser implementadas.

Es importante que las instituciones financieras comprendan estas amenazas y vulnerabilidades y tomen medidas proactivas para mitigar los riesgos. Esto incluye la implementación de estrategias de ciberseguridad sólidas, la formación de empleados y la colaboración con expertos en seguridad cibernética.

Tabla 6.. Afectaciones dentro de las instituciones financieras.

Problemas - Vulnerabilidades	**Clasificación Amenazas**
Fallas en la Seguridad del Software	Ciberataques Avanzados
Fallas en la Actualización de Software	Phishing y Spear Phishing
Fallas en la Autenticación y Autorización	Fraude en Transacciones Financieras
Falta de Encriptación	Acceso No Autorizado a Sistemas Críticos
Fuga de Datos	Ataques de Código Malicioso
Ataques de Inyección	Ransomware

En el contexto ecuatoriano, la ciberseguridad se ha convertido en un aspecto crucial para las instituciones financieras, dado el aumento de las amenazas cibernéticas y la creciente dependencia de la tecnología en el sector. Para garantizar la protección de los datos sensibles de los clientes y la integridad de las operaciones financieras, es esencial implementar métodos sólidos de ciberseguridad. A lo largo de este documento, se han analizado diversos métodos de protección que las instituciones financieras en Ecuador pueden adoptar para fortalecer su postura de ciberseguridad, hay tres puntos importantes los cuales deben ser especificados, ya que por lo que se ha tratado y escogido el tema:

En primer lugar, el establecimiento de una cultura de ciberseguridad dentro de la organización resulta fundamental. Esto implica la capacitación constante de los empleados en prácticas de seguridad cibernética, la concienciación sobre las amenazas actuales y la promoción de la responsabilidad compartida en la protección de los activos digitales. Además, se debe asegurar

una adecuada segregación de funciones y limitar el acceso a sistemas y datos solo a personal autorizado, reduciendo así el riesgo de amenazas internas.

En segundo lugar, la implementación de soluciones tecnológicas robustas desempeña un papel crucial en la protección cibernética. Esto incluye el uso de firewalls avanzados, sistemas de detección y prevención de intrusiones, y soluciones de cifrado para proteger la confidencialidad de los datos. Asimismo, las instituciones financieras deben mantener sus sistemas y aplicaciones actualizados mediante parches de seguridad, lo que ayuda a mitigar vulnerabilidades conocidas.

En tercer lugar, la monitorización constante de la infraestructura tecnológica es esencial para detectar y responder rápidamente a posibles amenazas. La implementación de sistemas de análisis de comportamiento y de detección de anomalías puede alertar sobre actividades inusuales en tiempo real, permitiendo una respuesta temprana para minimizar el impacto de un ataque.

En cuarto lugar, la adopción de prácticas de autenticación sólidas es crucial para evitar el acceso no autorizado a sistemas y datos sensibles. La autenticación de dos factores (2FA) o la autenticación multifactorial (MFA) añaden una capa adicional de seguridad al requerir información adicional más allá de las contraseñas tradicionales.

En resumen, la protección de la ciberseguridad en las instituciones financieras ecuatorianas requiere un enfoque integral que combine la formación del personal, la implementación de soluciones tecnológicas avanzadas, la monitorización constante y la aplicación de prácticas sólidas de autenticación. La colaboración con expertos en ciberseguridad y el seguimiento de las regulaciones y mejores prácticas locales e internacionales son esenciales para mantenerse al día con las amenazas en constante evolución y garantizar la confianza de los clientes en el sector financiero.

7. REFERENCIAS

Adelmann, F., Elliott, J., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, T., Morozova, A., Schwarz, N. & Wilson, C. (2020). *Cyber Risk and Financial Stability: It'sa Small World After All*.

Aftabi, S. Z., Ahmadi, A. & Farzi, S. (2023). Fraud detection in financial statements using data mining and GAN models. *Expert Systems with Applications*, *227*, 120144. https://doi.org/https://doi.org/10.1016/j.eswa.2023.120144

Aguirre Sánchez, M. J. (2021). *Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20566

Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J. & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, 100452. https://doi.org/https://doi.org/10.1016/j.cosrev.2021.100452

Alawida, M., Omolara, A. E., Abiodun, O. I. & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10, Part A), 8176–8206. https://doi.org/https://doi.org/10.1016/j.jksuci.2022.08.003

Alcívar-Cruz, B. & Llerena-Izquierdo, J. (2023). After-Sales and Customer Loyalty Strategies for Fixed Internet Through the Implementation of Virtual Assistance in the Ecuadorian Context. In V. Robles-Bykbaev, J. Mula & G. Reynoso-Meza (Eds.), *Intelligent Technologies: Design and Applications for Society* (pp. 139–149). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-24327-1_12

Amarullah, A. H., Runturambi, A. J. S. & Widiawan, B. (2021). Analyzing Cyber Crimes during COVID-19 Time in Indonesia. *2021 3rd International Conference on Computer Communication and the Internet (ICCCI)*, 78–83. https://doi.org/10.1109/ICCCI51764.2021.9486775

Analytica, O. (2018). Cybersecurity risks will rise in Mexico. *Emerald Expert Briefings*, *oxan-db*.

Ao, L. (2023). Data Storage Architecture and Data Backup Scheme for Digital Learning Platform. *2023 IEEE International Conference on Control, Electronics and Computer Technology (ICCECT)*, 1211–1215. https://doi.org/10.1109/ICCECT57938.2023.10140239

Aparicio, A., Martínez-González, M. M. & Cardeñoso-Payo, V. (2023). App-based detection of vulnerable implementations of OTP SMS APIs in the banking sector. *Wireless Networks*. https://doi.org/10.1007/s11276-023-03455-w

Bagheri, S., Ridley, G. & Williams, B. (2023). Organisational Cyber Resilience: Management Perspectives. *Australasian Journal of Information Systems*, *27*(0 SE-Research Articles). https://doi.org/10.3127/ajis.v27i0.4183

Cabrera, X. E. O. & Galarza, M. D. Á. (2022). Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. *Polo Del Conocimiento: Revista Científico-Profesional*, *7*(3), 16.

Carballo, D. H. & Villagran Gómez, I. A. (2023). *Análisis de ciberseguridad y nivel de madurez de los institutos de enseñanza salesianos del Uruguay*.

Catota, F. E., Morgan, M. G. & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, *4*(1), tyy002.

Catota, F. E., Morgan, M. G. & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), tyz001.

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q. & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1), 1–10.

Coello Ochoa, I. N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. http://dspace.ups.edu.ec/handle/123456789/20738

Dasgupta, S., Yelikar, B. V, Ramnarayan, Naredla, S., Ibrahim, R. K. & Alazzam, M. B. (2023). AI-Powered Cybersecurity: Identifying Threats in Digital Banking. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2614–2619. https://doi.org/10.1109/ICACITE57410.2023.10182479

Demertzi, V., Demertzis, S. & Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. *Applied Sciences*, *13*(2), 790.

Diaz Jimenez, C. D., Ariza Rodriguez, E., Ruiz Moncada, M. Y. & others. (2023). *La Ciberseguridad en las Pymes* [{B.S.} thesis]. Universidad EAN.

Díaz Redondo, R. P., Caeiro Rodríguez, M., López Escobar, J. J. & Fernández Vilas, A. (2021). Integrating micro-learning content in traditional e-learning platforms. *Multimedia Tools and Applications*, *80*(2), 3121–3151. https://doi.org/10.1007/s11042-020-09523-z

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, *5*(1), tyz013.

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica*. http://dspace.ups.edu.ec/handle/123456789/20576

García Wirton, C. (2021). *Ciberseguridad en el Sector Financiero ¿Cómo transformar una amenaza en una oportunidad?*

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E. & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, *121*, 102583. https://doi.org/https://doi.org/10.1016/j.technovation.2022.102583

Gulyás, O. & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, *219*, 84–90. https://doi.org/https://doi.org/10.1016/j.procs.2023.01.267

Gümüşboğa, Z. Ş. & Duruk, G. (2023). Comparison of effectiveness of different training tools on the level of knowledge about emergency management of avulsed teeth in non-dentists. *DIGITAL HEALTH*, *9*, 20552076231192148. https://doi.org/10.1177/20552076231192148

Haruna, W., Aremu, T. A. & Modupe, Y. A. (2022). *Defending against cybersecurity threats to the payments and banking system*.

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204.

Herrera Luque, F. J., Munera López, J. & Williams, P. (2021). Cyber risk as a threat to financial stability. *Revista de Estabilidad Financiera/Banco de España, 40 (Primavera 2021), p. 181-205*.

Humayun, M., Jhanjhi, N. Z., Alsayat, A. & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117. https://doi.org/https://doi.org/10.1016/j.eij.2020.05.003

Ife, C. C., Shen, Y., Murdoch, S. J. & Stringhini, G. (2021). Marked for Disruption: Tracing the Evolution of Malware Delivery Operations Targeted for Takedown. *Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses*, 340–353. https://doi.org/10.1145/3471621.3471844

Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., Khan, J. A., Rehman, A. U. & Shafiq, M. (2022). Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models. In *Sustainability* (Vol. 14, Issue 14). https://doi.org/10.3390/su14148374

Kalogiannidis, S., Paschalidou, M., Kalfas, D. & Chatzitheodoridis, F. (2023). Relationship between Cyber Security and Civil Protection in the Greek Reality. *Applied Sciences*, *13*(4), 2607.

Kang, Y. (2023). Development of Large-Scale Farming Based on Explainable Machine Learning for a Sustainable Rural Economy: The Case of Cyber Risk Analysis to Prevent Costly Data Breaches. *Applied Artificial Intelligence*, *37*(1), 2223862.

Kaoudi, Z. & Quiané-Ruiz, J.-A. (2022). Unified Data Analytics: State-of-the-Art and Open Problems. *Proc. VLDB Endow.*, *15*(12), 3778–3781. https://doi.org/10.14778/3554821.3554898

Karim, Y. & Hasan, R. (2021). *Taming the Digital Bandits: An Analysis of Digital Bank Heists and a System for Detecting Fake Messages in Electronic Funds Transfer BT - National Cyber Summit (NCS) Research Track 2020* (K.-K. R. Choo, T. Morris, G. L. Peterson, & E. Imsand, Eds.; pp. 193–210). Springer International Publishing.

Karimi, S., Ahmadi Malek, F., Yaghoubi Farani, A. & Liobikienė, G. (2023). The Role of Transformational Leadership in Developing Innovative Work Behaviors: The Mediating Role of

Employees’ Psychological Capital. In *Sustainability* (Vol. 15, Issue 2). https://doi.org/10.3390/su15021267

Kaur, G., Habibi Lashkari, Z. & Habibi Lashkari, A. (2021). *Cybersecurity Threats in FinTech BT - Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends* (G. Kaur, Z. Habibi Lashkari, & A. Habibi Lashkari, Eds.; pp. 65–87). Springer International Publishing. https://doi.org/10.1007/978-3-030-79915-1_4

Kelli, V., Sarigiannidis, P., Argyriou, V., Lagkas, T. & Vitsas, V. (2021). A Cyber Resilience Framework for NG-IoT Healthcare Using Machine Learning and Blockchain. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC42927.2021.9500496

Kim, K., Alfouzan, F. A. & Kim, H. (2021). Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework. In *Applied Sciences* (Vol. 11, Issue 16). https://doi.org/10.3390/app11167738

Lakshmi, K. L., S.Shobana, Kumar, B. P., K.B.Glory, Kumar, B. K. & Rani, S. (2023). Machine Learning based Cybersecurity Technique for Detection of Upcoming Cyber Attacks. *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, 621–625. https://doi.org/10.1109/ICCES57224.2023.10192738

Lee, C. & Lee, S. (2023). Overcoming the DDoS Attack Vulnerability of an ISO 19847 Shipboard Data Server. *Journal of Marine Science and Engineering*, *11*(5), 1000.

Lehmann, J., Schorz, S., Rache, A., Häußermann, T., Rädle, M. & Reichwald, J. (2023). Establishing Reliable Research Data Management by Integrating Measurement Devices Utilizing Intelligent Digital Twins. In *Sensors* (Vol. 23, Issue 1). https://doi.org/10.3390/s23010468

Linkov, I. & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber Resilience of Systems and Networks*, 1–25.

Linkov, I., Ligo, A., Stoddard, K., Perez, B., Strelzoffx, A., Bellini, E. & Kott, A. (2023). Cyber Efficiency and Cyber Resilience. *Communications of the ACM*, *66*(4), 33–37.

Malinka, K., Hujňák, O., Hanáček, P. & Hellebrandt, L. (2022). E-Banking Security Study—10 Years Later. *IEEE Access*, *10*, 16681–16699. https://doi.org/10.1109/ACCESS.2022.3149475

Mat, S. R. T., Ab Razak, M. F., Kahar, M. N. M., Arif, J. M., Mohamad, S. & Firdaus, A. (2021). Towards a systematic description of the field using bibliometric analysis: malware evolution. *Scientometrics*, *126*(3), 2013–2055. https://doi.org/10.1007/s11192-020-03834-6

Mayorga Muñoz, C. J. (2022). *Amenazas en el espacio cibernético con incidencia en la información de entidades públicas y privadas*.

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J. & Buchanan, W. J. (2022). Ransomware: Analysing the Impact on Windows Active Directory Domain Services. In *Sensors* (Vol. 22, Issue 3). https://doi.org/10.3390/s22030953

Melendrez-Caicedo, G. & Llerena-Izquierdo, J. (2022). Secure Data Model for the Healthcare Industry in Ecuador Using Blockchain Technology. *Smart Innovation, Systems and Technologies*, *252*, 479–489. https://doi.org/10.1007/978-981-16-4126-8_43

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G. & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: a systematic review. *Annals of Telecommunications*, *76*, 255–270.

Miller, T., Staves, A., Maesschalck, S., Sturdee, M. & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, *35*, 100464. https://doi.org/https://doi.org/10.1016/j.ijcip.2021.100464

Molina Castaño, S. (2021). *Ciberseguridad de las empresas financieras*.

Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S. & Syerov, Y. (2023). Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. In *Big Data and Cognitive Computing* (Vol. 7, Issue 2). https://doi.org/10.3390/bdcc7020093

Nambiar, A. & Mundra, D. (2022). An Overview of Data Warehouse and Data Lake in Modern Enterprise Data Management. In *Big Data and Cognitive Computing* (Vol. 6, Issue 4). https://doi.org/10.3390/bdcc6040132

Nawa, E.-L., Chitauro, M. & Shava, F. B. (2021). Assessing Patterns of Cybercrimes Associated with Online Transactions in Namibia Banking Institutions' Cyberspace. *2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, 1–6. https://doi.org/10.1109/IMITEC52926.2021.9714697

Nieto Rodríguez, C. O. & Sánchez Rojas, A. L. (2023). *Riesgos cibernéticos en el sector financiero colombiano situación actual y tendencias*.

Noel, S., Swarup, V. & Johnsgard, K. (2023). Optimizing network microsegmentation policy for cyber resilience. *The Journal of Defense Modeling and Simulation*, *20*(1), 57–79.

Ouafiq, E. M., Saadane, R. & Chehri, A. (2022). Data Management and Integration of Low Power Consumption Embedded Devices IoT for Transforming Smart Agriculture into Actionable Knowledge. In *Agriculture* (Vol. 12, Issue 3). https://doi.org/10.3390/agriculture12030329

Ozdemir, S., Wynn, M. & Metin, B. (2022). Cybersecurity and Country of Origin: Towards a New Framework for Assessing Digital Product Domesticity. *Sustainability*, *15*(1), 87.

Park, J., Jeon, C., Minn, D., Roh, H. & Sim, J.-Y. (2023). A 6.5nW, -73.5dBm Sensitivity, Cryptographic Wake-Up Receiver with a PUF-based OTP and Temperature-Insensitive Code Recovery. *2023 IEEE Symposium on VLSI Technology and Circuits (VLSI Technology and Circuits)*, 1–2. https://doi.org/10.23919/VLSITechnologyandCir57934.2023.10185235

Pavão, J., Bastardo, R. & Rocha, N. P. (2023). Cyber Resilience and Smart Cities, a Scoping Review. *2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6.

Pérez González, R. F. (2021). *Softwares de penetración utilizados por los piratas informáticos: Una revisión sistemática (2015-2020)*.

Quezada-Sarmiento, P. A., Alban-Cartuche, O. H., López-Pilataxi, L. E., Gonzaga-Tillaguango, H. F., Espinosa-Lara, E. P. & Ludeña-Reyes, A. P. (2023). Factores de riesgo, amenazas, vulnerabilidades y defensa en aplicaciones web turisticas. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E56*, 104–112.

Rameem Zahra, S., Ahsan Chishti, M., Iqbal Baba, A. & Wu, F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal*, *23*(2), 197–214. https://doi.org/https://doi.org/10.1016/j.eij.2021.12.003

Ramírez, F. C., Osorio, D. & Yanquen, E. (2017). *¿Qué es el riesgo cibernético y por qué es relevante para la estabilidad financiera?*

Rea-Guaman, A. M., Mejía, J., San Feliu, T. & Calvo-Manzano, J. A. (2020). AVARCIBER: A framework for assessing cybersecurity risks. *Cluster Computing*, *23*, 1827–1843.

Recalde Monar, J. A. (2021). *El ciberacoso por redes sociales en el Ecuador*. http://dspace.ups.edu.ec/handle/123456789/20945

Reyes Sarmiento, M. A. (2022). *Modelo de seguridad y transparencia bancaria para transferencias basado en tecnología Blockchain*.

Reyes Sarmiento, T. P. (2022). *Modelo de optimización de procesos bancarios o financieros para agilizar procedimientos relacionados mediante Business Intelligence*.

Reyes-Mena, F. X., Fuertes-Díaz, W. M., Guzmán-Jaramillo, C. E., Pérez-Estévez, E., Bernal-Barzallo, P. F. & Villacís-Silva, C. J. (2018). Application of business intelligence for analyzing vulnerabilities to increase the security level in an academic CSIRT. *Revista Facultad de Ingeniería*, *27*(47), 21–29.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V. & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, *23*(8), 4060.

Salguero Dorokhin, É., Fuertes, W., Lascano, E. & others. (2019). On the development of an optimal structure of tree parity machine for the establishment of a cryptographic key. *Security and Communication Networks*, *2019*.

Sánchez Castillo, A. F. & others. (2023). *Gestión de la ciberseguridad en el teletrabajo para pymes en colombia*.

Sánchez Peña, D. A. & others. (2023). *Ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia*.

Sanchez-Romero, J. & Llerena-Izquierdo, J. (2023). Revisión de la literatura sobre el uso del aprendizaje profundo enfocado en sistemas de inspección ópticos automatizados para la detección de defectos superficiales en el sector de la manufactura. *Revista InGenio*, *6*(2), 1–19. https://doi.org/10.18779/ingenio.v6i2.680

Smith, K. T., Smith, L. M., Burger, M. & Boyle, E. S. (2023). Cyber terrorism cases and stock market valuation effects. *Information & Computer Security*.

Smith, S. (2023). Towards a scientific definition of cyber resilience. *International Conference on Cyber Warfare and Security*, *18*(1), 379–386.

Tacuri López, I. L. (2021). *Acoso por medio de las tecnologías en las redes sociales durante tiempos de pandemia en Ecuador, una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20242

Terán Villafuerte, B. J. (2023). *Análisis de delitos informáticos relevantes en organizaciones gubernamentales de Latinoamérica*.

Toala Indio, Y. I. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio*.

Tsai, C.-P., Chang, C.-W., Hsiao, H.-C. & Shen, H. (2022). The Time Machine in Columnar NoSQL Databases: The Case of Apache HBase. In *Future Internet* (Vol. 14, Issue 3). https://doi.org/10.3390/fi14030092

Tsymbal, B., Kuzmenko, S., Huseynov, I. & Dobkina, K. (2023). *Institutional systems of public administration of personal security*.

Urgell, J. A. Z., Nieves, S. G., Becerra, A. G., Toledo, I. A. & Rodríguez, A. I. C. (2023). Análisis de la ciberseguridad en el sector financiero de México con el fin de implementar la metodología Zero trust y mejorarla. *Ciencia Latina Revista Científica Multidisciplinar*, *7*(1), 3384–3408.

Velicheti, S. S., Pavan, A. S. H., Reddy, B. T., Srikala, N. V, Pranay, R. & Kannaiah, S. K. (2023). The Hustlee Credit Card Fraud Detection using Machine Learning. *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, 139–144. https://doi.org/10.1109/ICCMC56507.2023.10084063

Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. *Business Horizons*, *64*(6), 787–797. https://doi.org/https://doi.org/10.1016/j.bushor.2021.07.014

Winker, T., Groppe, S., Uotila, V., Yan, Z., Lu, J., Franz, M. & Mauerer, W. (2023). Quantum Machine Learning: Foundation, New Techniques, and Opportunities for Database Research. *Companion of the 2023 International Conference on Management of Data*, 45–52. https://doi.org/10.1145/3555041.3589404

Yamini, K., Anitha, V., Polepaka, S., Chauhan, R., Varshney, Y. & Singh, M. (2023). An Intelligent Method for Credit Card Fraud Detection using Improved CNN and Extreme Learning Machine. *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, 810–815. https://doi.org/10.1109/ICCES57224.2023.10192774

Zambrano, P., Torres, J., Tello-Oquendo, L., Jácome, R., Benalcázar, M. E., Andrade, R. & Fuertes, W. (2019). Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach. *IEEE Access*, *7*, 142129–142146.

Zerega-Prado, J. & Llerena-Izquierdo, J. (2022). Arquitectura de consolidación de la información para seguros de la salud mediante Big Data. *Memoria Investigaciones En Ingeniería*, *0*(23 SE-Artículos). https://doi.org/10.36561/ING.23.3