UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

El aumento del nivel de seguridad en los sistemas de información financieros de la banca ecuatoriana mediante el uso de tecnologías: Un mapeo sistemático

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: Carlos Andrés Rosero Martillo

TUTOR: Nelson Salomón Mora Saltos, Msig.

Guayaquil – Ecuador

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Carlos Andrés Rosero Martillo con documento de identificación N° 0926570110 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, 15 de abril del año 2023

Atentamente,

Carlos Andrés Rosero Martillo
C.I. 0926570110

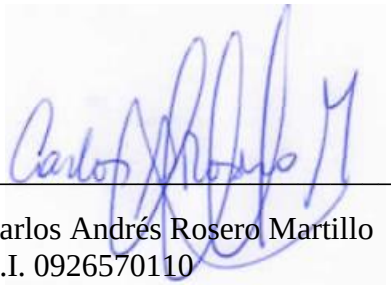
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Carlos Andrés Rosero Martillo con documento de identificación N° 0926570110, 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 del Artículo Académico: "**El aumento del nivel de seguridad en los sistemas de información financieros de la banca ecuatoriana mediante el uso de tecnologías: Un mapeo sistemático**", 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, 15 de abril del año 2023

Atentamente,



Carlos Andrés Rosero Martillo
C.I. 0926570110

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Nelson Salomón Mora Saltos, Msig. con documento de identificación N° 0909257800, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **El aumento del nivel de seguridad en los sistemas de información financieros de la banca ecuatoriana mediante el uso de tecnologías: Un mapeo sistemático**, realizado por Carlos Andrés Rosero Martillo con documento de identificación N° 0926570110, 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, 15 de abril del año 2023

Atentamente,

_____

Nelson Salomón Mora Saltos, Msig
C.I. 0909257800

DEDICATORIA

Dedico este trabajo primero a Dios por ser el inspirador que me ha dado fuerza para continuar esta dura travesía y poder así obtener uno de los anhelos más deseados, a mis padres Carlos y Narcisa que fueron el pilar fundamental para iniciar esta carrera universitaria, ellos me enseñaron que con esfuerzo y constancia todo se puede conseguir, a mi amada esposa Stefania que con su apoyo y confianza que me brinda día tras día me ayuda a ser mejor persona y profesional, a mi hija amada Romina, con cada abrazo y beso que me da, son la motivación necesaria para realizar este proyecto.

AGRADECIMIENTO

Agradezco a Dios por brindarnos el don de la vida por guiarnos en lo espiritual a lo largo de nuestra existencia, gracias a mis padres por ser los principales creyentes y promotores de nuestros sueños, por sus consejos de vida que al pasar el tiempo tienen tanta razón, a mis hermanos por su confianza y sus palabras de aliento, a mi familia por estar siempre junto a mi siendo mi inspiración diaria, finalmente quiero agradecer a mis grandes amigos por su amistad incondicional, en especial a mi gran amiga la Ing. Verónica Vargas que me dio luz con el presente proyecto.

RESUMEN

Los datos son activos invaluables en la industria financiera y la seguridad es un punto neurálgico. El objetivo general es identificar tecnologías para aumentar el nivel de seguridad de los sistemas de información financieros en la banca del Ecuador mediante la revisión de trabajos utilizando la técnica del mapeo sistemático. Se utiliza la técnica del mapeo sistemático y modelo PRISMA. Esta investigación pretende identificar aquellas tecnológicas que ayudan a aumentar el nivel de seguridad específicamente en los sistemas de información financieros en entidades bancarias. Entre los resultados obtenidos están: se identificaron 29 artículos científicos que utilizan tecnologías de seguridad en los sistemas de información financieros, se conocieron tipos de sistemas bancarios web, móvil, desktop; se obtuvo porcentajes de características como privacidad, seguridad, disponibilidad, integridad y confidencialidad; se conocieron tecnologías de seguridad utilizadas como blockchain, inteligencia artificial, certificados, algoritmos; se obtuvo los porcentajes de los servicios digitales de NIS2 y los problemas considerados en NIS 2; y entre los 29 artículos, el 48% de artículos son factibles para adopción e implementación y 52% no son factibles. Se concluye que en la seguridad de la información algunas de las tareas principales son la protección de datos personales, protección de servicios en línea, aumentar la seguridad de los datos en los bancos, esta investigación es un pequeño aporte para conocer la situación científica en esta área de negocios.

Palabras claves: Seguridad de la Información, Sistemas de Información Financieros, Mapeo Sistemático, Tecnologías Financieras.

ABSTRACT

Data is an invaluable asset in the financial industry and security is a pain center. The general objective is to identify technologies to increase the level of security of financial information systems in Ecuadorian banking by reviewing works using the technique of systematic mapping. The technique of systematic mapping and PRISMA model is used. This research aims to identify those technologies that help increase the level of security specifically in financial information systems in banks. Among the results obtained are: 29 scientific articles that use security technologies in financial information systems were identified, types of web, mobile, desktop banking systems were known; Percentages of characteristics such as privacy, security, availability, integrity and confidentiality were obtained; security technologies used as blockchain, artificial intelligence, certificates, algorithms were known; the percentages of NIS2 digital services and the problems considered in NIS 2 were obtained; and among the 29 articles, 48% of articles are feasible for adoption and implementation and 52% are not feasible. . It is concluded that in information security some of the main tasks are the protection of personal data, protection of online services, increase data security in banks, this research is a small contribution to know the scientific situation in this business area.

Key words: Information Security, Financial Information Systems, Systematic Mapping, Financial Technologies.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

Un entorno financiero permite canalizar servicios y recursos a las actividades productivas, así ahorristas se conectan con inversionistas mediante sistemas de información; las empresas y personas buscan financiamiento para planes de producción o generación de empleos, además de otros servicios que se ofrece en el sistema financiero que tienen las entidades de servicios financieros, capitalización, aseguradoras, entidades de crédito o bancos (Salas et al., 2020). En la industria financiera, "los datos son activos invaluables", gran parte de las adquisiciones de los inversionistas obedece a la "calidad de la información" que los sistemas de información web o escritorio o móvil entreguen a inversores, clientes, proveedores o terceros; las TIC cada vez modernizan los sistemas de información, negocios y transacciones, además crecen los datos y riesgos de la información; los sistemas bancarios ayudan a los clientes o proveedores en nuevas experiencias personalizadas, menor tarifa, mejores servicios, menor costo operativo, aumentar las ventajas competitivas, procesamiento de gran cantidad de transacciones, entre otros (Luo et al., 2020).

Los bancos tienen grandes volúmenes de datos que son importantes en la gestión de los clientes y sus transacciones, estos datos son analizados para optimizar la atención y tomar ventajas, en otro ámbito, estos datos deben ser protegidos desde varias aristas, mediante estrategias o herramientas tecnológicas para aumentar la seguridad interna y externa; los bancos tienen desafíos en varios ámbitos como predicción de ahorros, créditos, gestión de riesgos, y en especial la seguridad de los datos/sistemas/infraestructura (Dawood et al., 2019).

A nivel de América Latina hay 66 ataques a bancos, el impacto a nivel de confidencialidad es 13%, en Integridad es 10% y en Disponibilidad es 77%, entre las causas están las vulnerabilidades en 30%, robo de credenciales en 29%, Phishing en 31% y Otras causas en 10%. De estos ataques, 3 pertenecen a Ecuador en bancos locales (Naciones-Unidas, 2021).

En Ecuador, el sistema financiero es una de las bases de la economía de nuestro país, y está formado por bancos, cooperativas y otras entidades que son controladas por instituciones de supervisión estatal (Cárdenas Muñoz et al., 2021). Los bancos privados tienen variedad de aplicaciones informáticas o sistemas de información que utilizan en sus canales digitales para banca móvil, banca en línea, ATM, puntos de venta, sucursales bancarias, corresponsales bancarios, corresponsales no bancarios y centros de atención (Malinka et al., 2022). De acuerdo a la Superintendencia de Bancos del Ecuador en el sistema financiero existen: almacenes de

depósitos, bancos off shore, bancos privados extranjeros/nacionales, buros crediticios, casas de cambios, compañías de titulación, gestión de tarjetas de crédito, entidades de seguro social, entidades financieras públicas (Superintendecia_de_Bancos Ecuador, 2022). Entre ellos hay 24 bancos privados que a través de sus sistemas informáticos dan servicios como: inversiones, fondos, interés, depósitos, créditos, entre otros; hasta mayo del 2022 la banca pública gestiona 52 mil millones en activos, 35 mil millones en cartera bruta, 41 mil millones en depósitos, 5 mil millones en patrimonio (ASOBANCA, 2022). Esta investigación está dirigida dar opciones tecnológicas que minimicen las vulnerabilidades del sistema de información financiero de un banco privado nacional.

En los sistemas de información financiero, existen varios problemas por resolver, como aumentar el rendimiento de la aplicación informática, mantener la estabilidad de los repositorios de los datos, mantener la escalabilidad de los servicios en las aplicaciones y datos (Luo et al., 2020), asegurar la autenticación para acceso a los datos y servicios bancarios (Incel et al., 2021).

De acuerdo a (Fadlallah et al., 2020) en una investigación sobre 150 sistemas informáticos en diferentes sectores determinaron que las vulnerabilidades están en la siguiente distribución: banca 10%, tecnologías 22%, ventas 21%, construcción 16%, salud/educación 10%, entretenimiento 10%, seguros 6% y gobierno 5%. Algunas seguridades en sistemas bancarios se aplican por medio de autenticación, autenticación entrelazada, integridad, anonimato del cliente y no repudio (Ahmed et al., 2021).

El fundamento legal para este proyecto se basa en la Ley de Datos Personales que en el Capítulo II Artículo 10 Literal J, especifica que los responsables de los datos personales deben aplicar medidas de seguridad técnicas para protegerlos contra amenazas, riesgos y vulnerabilidades (Asamblea-Nacional-del-Ecuador, 2021).

Esta investigación pretende identificar aquellas tecnológicas que ayudan a aumentar el nivel de seguridad específicamente en los sistemas de información financieros en entidades bancarias, las alternativas se buscan en artículos científicos para obtener propuestas frescas a nivel científico, por supuesto que algunas alternativas son científicas y aun puede que no se comercialicen, no se toman en cuenta los precios monetarios de las tecnologías encontradas.

El objetivo general es identificar tecnologías para aumentar el nivel de seguridad de los sistemas de información financieros en la banca del Ecuador mediante la revisión de trabajos utilizando la técnica del mapeo sistemático

Los objetivos específicos son:

- Identificar artículos científicos de relevancia que utilicen tecnologías de seguridad en los sistemas de información financieros para su clasificación mediante el uso de la técnica del mapeo sistemático.
- Analizar las tecnologías de seguridad utilizados en los sistemas de información financieros para elaborar una tabla categorizada basada en la normativa de la directiva NIS2.
- Evaluar los resultados encontrados para su contrastación y posible adopción en la banca del Ecuador mediante la elaboración de una tabla de porcentajes de factibilidad.

Este documento se describe en los siguientes capítulos: el siguiente capítulo describe la revisión de la literatura describe los conceptos de Directva NIS 2, tecnología financiera, las amenazas, vulnerabilidades o ataques en sistemas informáticos, además se describe ciertas medidas de seguridad aplicadas en sistemas de información financiero, aquí algunos se basan en inteligencia artificial, blockchain y otros. Otro capítulo describe la metodología aplicada en cada uno de los objetivos específicos. El capítulo Resultados describe los datos obtenidos en el mapeo sistemático, las tecnologías de seguridad encontradas en la literatura y una evaluación de los artículos obtenidos en el mapeo sistemático. El ultimo capitulo describe las discusiones y conclusiones.

2. REVISIÓN DE LITERATURA

2.1. NIS 2

NIS 2 es la segunda versión de Security of Network and Information Systems, es una norma de la unión europea sobre ciberseguridad que proporciona medidas legales para los paises europeos. La Directiva NIS 2 mejora las características ciberseguridad y pide designación de autoridades en esta rama; genera mejor cooperación e intercambio de información; y estratégica y operativa; y mejora la resiliencia cibernética de toda empresa en siete áreas (agua potable, banca, energía, infraestructuras del mercado financiero, infraestructuras digitales, transporte y salud) y en tres servicios digitales (mercados en línea, motores de búsqueda y servicios de computación en la nube), esto exige que los operadores/proveedores de servicios digitales determinen precisiones de ciberseguridad y notificación de incidentes. Esta directiva evalúa el impacto de ciberseguridad y los problemas como: el bajo nivel de resiliencia cibernética, la resiliencia inconsistente y bajo nivel de conciencia situacional. Por ejemplo, los hospitales de un país aplicaban la Directiva NIS y en otro país todos los hospitales si aplican la directiva (European Commission, 2020).

2.2. Tecnología Financiera

Son las Tecnologías de Información aplicadas o utilizadas en las diversas operaciones de empresas financieras para mejorar la calidad de los servicios; aquí se utilizan varias TI, análisis de datos, computación en la nube, redes, big data, procesamiento de diferentes tipos de datos; consiste en la digitalización de los amplios servicios financieros, aunque tiene desafíos de seguridad y privacidad en los sistemas informáticos (Mehrban et al., 2020).

El núcleo Tecnologías Financieras es el avance, interacción e integración de la industria financiera con las nuevas tecnologías; este concepto plantea la optimización o reconstrucción de los sistemas informáticos financieros, patrones, estructuras subyacentes y la lógica financiera, con estas características se abrevia el flujo de datos/información y fondos entre las instituciones financieras (Song et al., 2022).

2.3. Amenazas, vulnerabilidades o ataques en sistemas informáticos financieros

Existen ataques a los sistemas de información financiero en áreas como: autenticación (predicción de contraseñas, descifrado de contraseñas, re direccionamiento, suplantación de sitios, ataques simultáneos, ingeniería social, robo de credencial, robo de voz/rostro), robo de

identidad (sustracción de credenciales, vinculación sin autorización), ataque de comunicación (escucha pasiva, actualización de mensajes, descifrado de comunicación, incrustación en la web), ataques directos al banco (ataques internos, ataques entre bancos, engaño a empleados, malware, ransomware, ataque al servidor, denegación de solicitudes) (Malinka et al., 2022).

Otros diferentes tipos de amenazas en sistemas financieros móviles como: dispositivo, red y centro de datos. En ataques: búsqueda de puertos, rastreadores de datos (tarjetas de crédito o contraseñas), decodificación de archivos, código troyano. Existen amenazas en las aplicaciones móviles como: escritura de aplicaciones en archivos de terceros, validación en la identificación del host, sensibilidad en la ejecución remota, falta ocultar el programa fuente, falta de configuración correcta, cifrar toda solicitud (Yildirim & Varol, 2019).

Otros ciberataques son ataques a la privacidad, robos de datos, accesos ilegítimos, ataques al método de autenticación, ataques a la confidencialidad de los clientes, ataques a la integridad de los datos que pertenecen a los clientes, ataques a la disponibilidad de los servicios que ofrece el banco (Ahmed et al., 2021).

2.4. Seguridades en sistemas de información financiero

En (Incel et al., 2021) se utiliza algoritmos de clasificación en Inteligencia Artificial como SVM, kNN, MLP, RF y Bayes, para aumentar la seguridad en la autenticación al entrar a sistemas de información móvil, la autenticación se aplica mediante una biometría de comportamiento y toma datos de la pantalla y sensores del teléfono inteligente para analizarla con los algoritmos.

En (Luo et al., 2020) proponen un modelo que utiliza Aprendizaje Automático en los procesos de depósitos/préstamos en sistema de información en línea, además baja la carga de transacciones y aumenta la seguridad en las transacciones.

En (Malinka et al., 2022) se describen varios métodos de autenticación en sistemas bancarios, que cumplen estándares europeos y su fuerza ante los ataques, se centran en las aplicaciones en línea, unas aplicaciones utilizan combinación de contraseñas con pin o con token o biometría.

En (S. Y. Jin & Xia, 2022) se propone un framework basado en blockchain para verificación de moneda digital, este marco es general y regulatorio, es decir puede servir para economías de

varios países, los algoritmos son divididos para ajustarse a las operaciones de los diferentes bancos.

En (Song et al., 2022) se propone una arquitectura basada en blockchain, esta arquitectura tiene cuatro niveles: nube, internet, blockchain y sistemas informáticos; los dispositivos están conectados a la nube mediante un certificado, el nivel blockchain está formado por contratos inteligentes, reglas de negocios y códigos, esta tecnología asegura las transacciones mediante cifrado, estados y almacenamiento distribuido.

En sistemas informáticos móviles se propone: utilizar certificados digitales que sean encriptados, guardar los datos de la sesión del cliente, aumentar factores en el inicio de sesión, cambio de letras y números en las sesiones, aumento de combinación en usuario y contraseña, otros factores de autenticación. En sistemas informáticos en línea se propone: utilizar memoria del navegador web para localizar código malo, registro e identificación del dispositivo, utilizar identificación secreta, análisis de transacciones bancarias mediante inteligencia artificial (Yildirim & Varol, 2019).

En (Dumitrescu et al., 2022) se propone un método para localizar nodos que generen transacciones con anomalías, el método analiza los datos como la moneda, hora de la transacción, modalidades, fondos de la cuenta de origen o destino; este método antifraude se opera en el sistema informático que genera la transacción para dar aviso al banco sobre posibles transacciones dudosas, y enfrentar lavado de dinero en escenarios complejos.

En (Kumar et al., 2020) se discute un método para aumentar la seguridad de las aplicaciones web en la etapa de desarrollo para minimizar los costos, anular duplicación de actividades y aumentar la vida útil de una aplicación segura; el método es cuantitativo para determinar la seguridad de una aplicación web.

En (Ahmed et al., 2021) se realiza una descripción de tecnologías y métodos para dar seguridad a aplicaciones móvil bancaria, como cifrado de claves, autenticación por firma, autenticación por certificado, firewall en redes, diferentes tipos de autenticación y pin.

3. METODOLOGÍA

Para el primer objetivo: "Identificar artículos científicos de relevancia que utilicen tecnologías de seguridad en los sistemas de información financieros para su clasificación mediante el uso de la técnica del mapeo sistemático". Se utiliza la técnica del mapeo sistemático utilizada en (Ramírez & Mora, 2021) para determinar las fases y preguntas de investigación relacionadas a tecnologías en seguridad de la información o seguridad digital en cualquier plataforma financiera, la revisión tiene 4 fases representadas en la figura 1.

A continuación se describen las fases a realizar:

Fase 1: Delimitación de las preguntas de investigación: Se plantean 4 preguntas:

a) ¿Cuáles son los tipos de sistemas de información o aplicaciones informáticas en la industria bancaria?

b) ¿Cuáles son las características de las tecnologías en seguridad?

c) ¿Cuáles son las tecnologías de seguridad digital o seguridad de información en la industria bancaria?

d) ¿Aplica en una de las áreas estratégicas consideradas en NIS 2 (agua potable, banca, energía, infraestructuras del mercado financiero, infraestructuras digitales, transporte y salud)?

e) ¿Aplica en uno de los servicios digitales considerados en NIS 2 (mercados en línea, motores de búsqueda y servicios de computación en la nube)?

f) ¿Existe uno de los problemas considerados en NIS2 (bajo nivel de resiliencia cibernética, resiliencia inconsistente o bajo nivel de conciencia situacional)?

Fase 2: Realizar la búsqueda bibliográfica: Se plantea buscar en las bibliotecas virtuales que la Universidad Politécnica Salesiana entrega acceso a los estudiantes y docentes, las bibliotecas son IEEE Xplore, ACM Digital Library y Springer. Las palabras claves de búsqueda son "Security System Banking", "Security Banking", "Technology Banking".

Fase 3: Seleccionar los documentos: Se aplican criterios de inclusión y exclusión que filtran los artículos direccionados a responder las preguntas de investigación

Tabla 1. Criterios de selección

Inclusión	Exclusión
Desde año 2018 al 2022	Documentos duplicados
Idioma inglés o español	Documentos de solo resumen
Relacionados a seguridad en aplicaciones informáticas	Documentos no relacionados
Propuestas teóricas o implementadas	Libros

Fuente: Autor.

Fase 4: Análisis de los documentos: Se realiza en el desarrollo del artículo, los documentos seleccionados se tabulan en una hoja electrónica con las características de las tecnologías.

Figura 1. Mapeo Sistemático

Para el segundo objetivo, Analizar las tecnologías de seguridad utilizados en los sistemas de información financieros para elaborar una tabla categorizada basada en la normativa de la directiva NIS2. Se analizan las tecnologías apropiadas para el sistema de información financiera, se utiliza la hoja electrónica para tabular los artículos científicos en estándares de seguridad, tipos de sistemas de información, características generales y tecnologías en seguridad de información. Se categorizan los artículos científicos en las características de NIS 2 (Security of Network and Information Systems), si aplica en una de las áreas (agua potable, banca, energía, infraestructuras del mercado financiero, infraestructuras digitales, transporte y salud), si aplica en uno de los servicios digitales (mercados en línea, motores de búsqueda y servicios de computación en la nube), si existe uno de los problemas como: bajo nivel de resiliencia cibernética, resiliencia inconsistente o bajo nivel de conciencia situacional (European Commission, 2020).

Para el tercer objetivo, Evaluar los resultados encontrados para su contrastación y posible adopción en la banca del Ecuador mediante la elaboración de una tabla de porcentajes de factibilidad. No todas las características NIS2 o tecnologías encontradas son aplicables a la

banca financiera local, para confirmar si cada artículo y su tecnología es apropiado en nuestro entorno ecuatoriano, se consideran todas las características NIS2 y propiedades de las tecnologías en seguridad que se encuentran en la hoja electrónica, si el puntaje del documento es mayor al puntaje promedio de todos los artículos entonces se considera el porcentaje de factibilidad del artículo para nuestro entorno ecuatoriano.

4. RESULTADOS

4.1. Identificación de artículos científicos de relevancia que utilicen tecnologías de seguridad en los sistemas de información financieros para su clasificación mediante el uso de la técnica del mapeo sistemático

El mapeo sistemático se plasma en un modelo PRISMA que ayuda en el filtrado y selección de artículos científicos de las bibliotecas IEEE, ACM y Springer; se recolectaron y seleccionaron 84 artículos, luego se removió un artículo por ser duplicado, se removió 17 artículos por no ser elegibles es decir no tratan sobre tecnologías financieras ni seguridad, se removió 19 artículos por otras razones es decir tienen otras directrices. Luego quedaron 47 artículos y se excluyeron 6 por ser artículos solo teóricos y no presentan arquitecturas o modelos. Luego quedaron 41 artículos y se procedió a realizar la recuperación del contenido completo o documento PDF, pero 7 artículos no es posible bajarlos. Luego quedaron 34 artículos y se excluyeron 2 artículos por ser contenido diferente al idioma ingles y 3 artículos se excluyeron por ser solo artículos resumen. Finalmente 29 artículos son la base para la lectura integra y análisis para contestar las preguntas de investigación, ver Fig. 2.

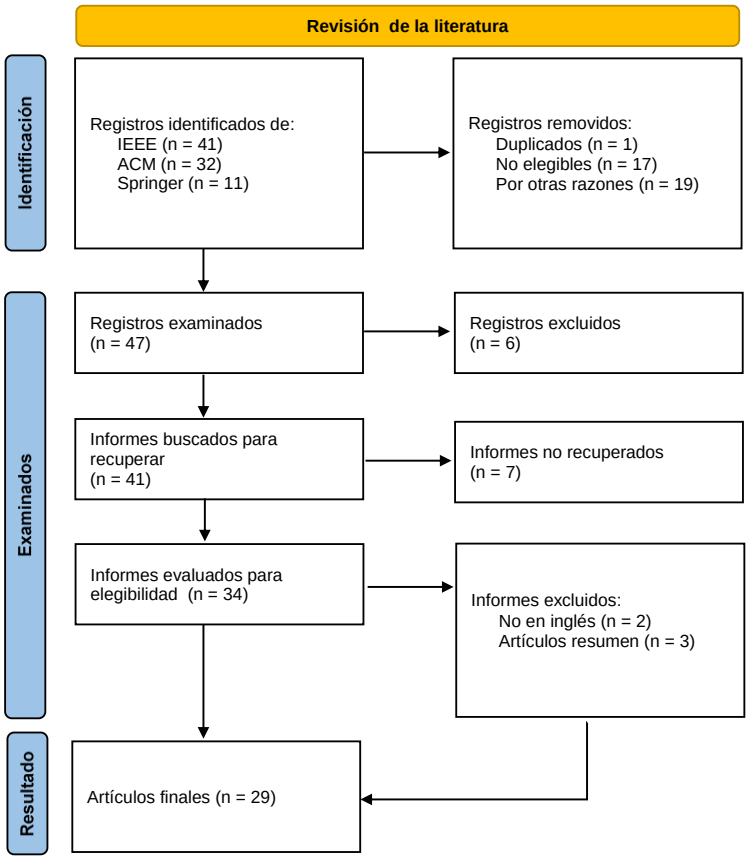


Figura 2. PRISMA.

Los artículos científicos que están seleccionados se presentan en la tabla 1, se encuentran agrupados por biblioteca.

Tabla 2. Referencias seleccionadas

Biblioteca	Artículos
IEEE	(Kumar et al., 2020), (Yildirim & Varol, 2019), (Dumitrescu et al., 2022), (S. Y. Jin & Xia, 2022), (Incel et al., 2021), (Malinka et al., 2022), (Dawood et al., 2019), (Salas et al., 2020), (Fadlallah et al., 2020), (Luo et al., 2020), (Song et al., 2022), (Ahmed et al., 2021), (Mehrban et al., 2020), (Kwon et al., 2019), (Chen et al., 2021)
ACM	(Nasir et al., 2021), (T. Jin et al., 2019), (Huebner et al., 2019), (Luz & Farias, 2020), (Bambang Triantono & Priyatiningsih, 2020), (Kurmanova et al., 2021), (Cao, 2021), (Wang et al., 2021), (Chowdhury et al., 2022)
Springer	(Choi & Lee, 2018), (Obaid et al., 2019), (Tay & Mourad, 2020), (Ileberi et al., 2021), (Fan et al., 2018)

Fuente: Autor.

4.2. Analizar tecnologías de seguridad utilizados en los sistemas de información financieros para elaborar una tabla categorizada basada en la normativa de la directiva NIS2

En este objetivo se responden las preguntas de investigación que fueron planteadas en la metodología.

a) ¿Cuáles son los tipos de sistemas de información o aplicaciones informáticas en la industria bancaria? Se clasificó 3 tipos de sistemas de información que utiliza la industria bancaria en sistema web, sistema de escritorio y sistema móvil; entre los 29 artículos sólo 25 si expresan que utilizan alguno de estos tipos de sistemas, y 4 documentos no expresan que tipo de sistema utilizan; entre los 25 documentos el 48% utiliza sistema web, 45% utiliza sistema móvil y 7% utiliza sistema de escritorio. Es decir las propuestas apuntan al ambiente web y/o móvil, ver Fig. 3. Aquí 16 documentos nombran los sistemas web y móvil.

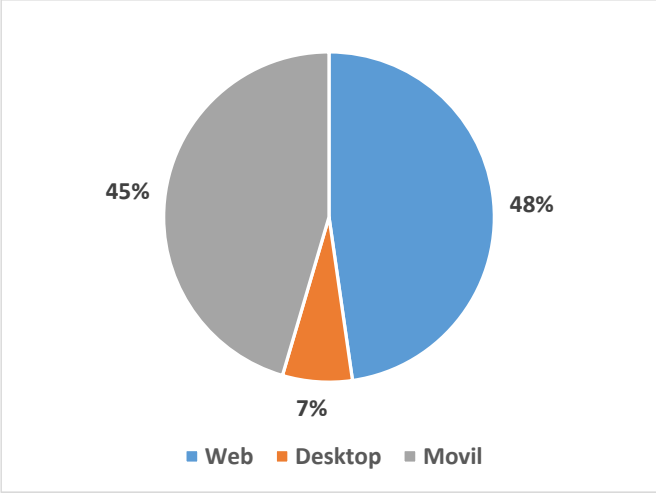


Figura 3. Tipos de sistemas de información.

b) ¿Cuáles son las características de las tecnologías en seguridad?

Como características de las tecnologías se hallaron la Confidencialidad, Integridad, Disponibilidad (CIA), Seguridad y Privacidad; entre los 29 artículos sólo 3 no nombran ninguna de estas características y 26 si nombran. Los 26 documentos nombran una o varias de estas características. En seguridad es 37%, en confidencialidad es 19%, en disponibilidad es 17%, en integridad es 14%, y en privacidad es 13%, ver Fig. 4. Aquí 8 documentos nombran CIA, y otros 8 documentos nombran seguridad-privacidad, y sólo 2 documentos nombran las cinco características.

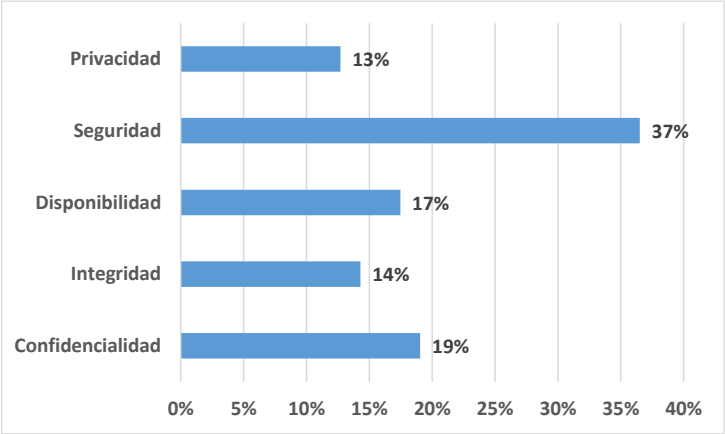


Figura 4. Características.

c) ¿Cuáles son las tecnologías de seguridad digital o seguridad de información en la industria bancaria?

Entre las tecnologías de seguridad se hallaron algoritmos diversos, monitoreo, autenticación, certificados digitales, Blockchain e Inteligencia Artificial (IA); entre los 29 artículos, sólo 1 no nombra ninguna forma de asegurar la información y los otros 28 si nombran uno o más tecnologías; algoritmos diversos en 29%, mecanismos de autenticación en 29%, IA en 22%, Blockchainen 10%, certificados digitales en 6% y herramientas de monitoreo en 4%, ver Fig. 5. Aquí, los certificados y autenticación se utilizan en 3 documentos; el monitoreo y autenticación se utilizan en 2 documentos; las propuestas en IA son independientes de las propuestas en Blockchain.

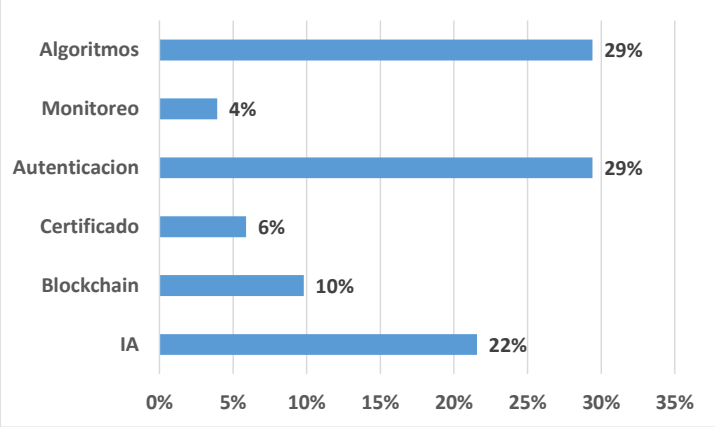


Figura 5. Tecnologías en seguridad de información.

d) ¿Aplica en una de las áreas estratégicas consideradas en NIS 2 (agua potable, banca, energía, infraestructuras del mercado financiero, infraestructuras digitales, transporte y salud)?

Entre las áreas estratégicas de NIS2 entre los 29 artículos, 4 son de áreas generales o no especificadas y los otros 25 aplican a la banca, ver Fig. 6. Aquí, los generales son el 14% y del sector bancario son el 86%; la búsqueda sistemática se orientó a artículos del área financiera o bancaria.

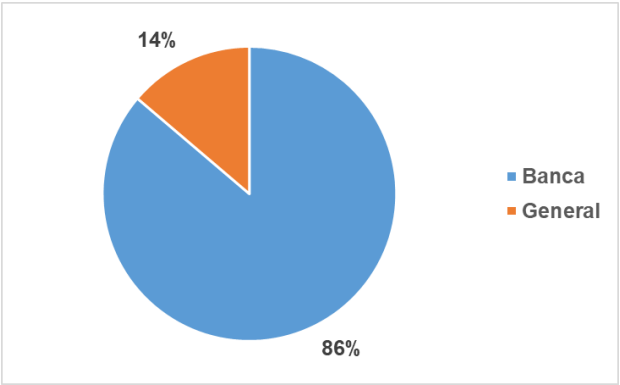


Figura 6. Áreas estratégicas NIS 2.

e) ¿Aplica en uno de los servicios digitales considerados en NIS 2 (mercados en línea, motores de búsqueda y servicios de computación en la nube)?

De los servicios digitales de NIS2 que ofrecen las propuestas entre los 29 artículos, 13% son de mercados en línea, 28% son de motores de búsqueda, y 59% ofrecen servicios de computación en la nube, ver Fig. 7. Aquí, las propuestas que ofrecen aplicaciones o sistemas bancarios utilizan los servicios y procesos ubicados en la nube.

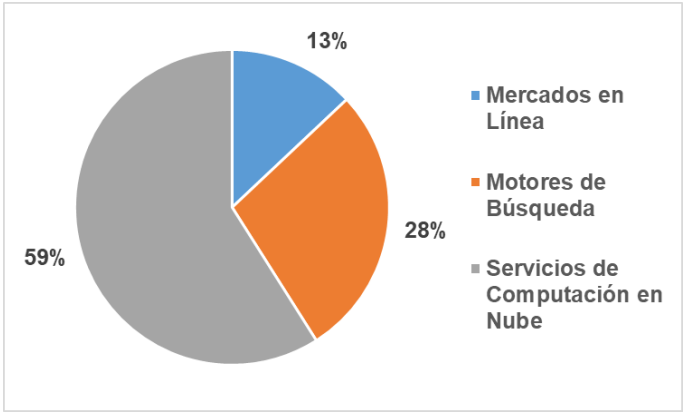


Figura 7. Servicios digitales NIS 2.

f) ¿Existe uno de los problemas considerados en NIS2 (bajo nivel de resiliencia cibernética, resiliencia inconsistente o bajo nivel de conciencia situacional)?

Entre los problemas considerados en NIS 2 se encontraron que: el 14% tiene problemas de conciencia es decir que las personas no consideran la seguridad de los datos; el 28% tienen resiliencia inconsistente es decir no hay coherencia en la capacidad de respuestas ante incidentes; el 58% tienen resiliencia cibernética es decir capacidad para imposibilitar incidentes de ciberseguridad y pronta recuperación. Ver Fig. 8.

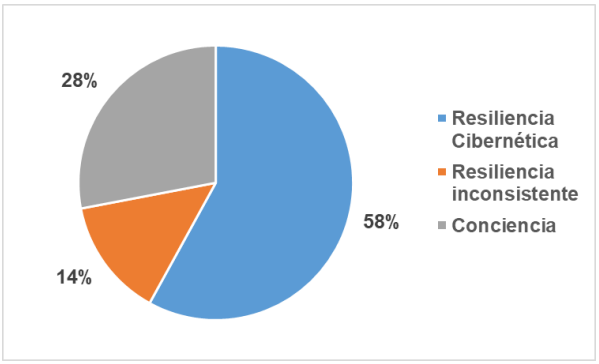


Figura 8. Problemas de NIS 2.

4.3. Evaluar los resultados encontrados para su contrastación y posible adopción en la banca del Ecuador mediante la elaboración de una tabla de porcentajes de factibilidad

No todas las tecnologías encontradas son aplicables a la banca financiera local, para evaluar si la tecnología es apropiada en nuestro entorno ecuatoriano, se consideran todas las propiedades y características de cada artículo obtenido en la revisión sistemática y se tabularon en una hoja electrónica de Microsoft Excel, las tecnologías obtenidas son Inteligencia Artificial (IA), Blockchain, Certificados, Autenticación, Monitoreo y Algoritmos. Por cada característica que

tenga un artículo se le asigna un punto, son 14 características cuantitativas (1-Web, 2-Desktop, 3-Móvil, 4-Confidencialidad, 5-Integridad, 6-Disponibilidad, 7-Seguridad, 8-Privacidad, 9-IA, 10-Blockchain, 11-Certificado, 12-Autenticación, 13-Monitoreo, 14-Algoritmos) y 3 son características cualitativas (15-Area Estratégica, 16-Servicios Digitales, 17-Problemas); por cada artículo se tiene la suma de los puntos sobre 14 en la columna *Puntación*, y porcentaje de puntuación en la columna *% de artículo* (Puntuación/14); la suma global de la columna *Puntación* es 158 puntos; el *Promedio Global* de la Puntación es 5.45 (158 puntos/29 artículos), esto equivale al *Porcentaje Global* que es 39% de las 14 características (5.45/14). Para determinar la *Factibilidad*, si la columna *% de artículo* es mayor e igual al *Porcentaje Global* (39%) entonces SI se considera apropiado para su posible adopción en la banca del Ecuador, ver Fig. 9.

		Tipo de SI			Caracteristicas					Tecnologias en SI						NIS 2					
No	Referencia	1-Web	2-Desktop	3-Movil	4-Confidencialidad	5-Integridad	6-Disponibilidad	7-Seguridad	8-Privacidad	9-IA	10-Blockchain	11-Certificado	12-Autenticacion	13-Monitoreo	14-Algoritmos	15-Area Estrategica	16-Servicios Digitales	17-Problemas	Puntuacion	% de artículo	FACTIBILIDAD
1	(Kumar et al., 2020)	X			X	X	X			X						General	ML	RC	5	36%	NO
2	(Yildirim & Varol, 2019)	X		X								X	X	X		Banca	MB	RI	5	36%	NO
3	(Dumitrescu et al., 2022)	X					X								X	Banca	CN	RC	3	21%	NO
4	(S. Y. Jin & Xia, 2022)							X	X		X	X	X		X	Banca	CN	CO	6	43%	SI
5	(Incel et al., 2021)			X				X		X			X			Banca	CN	RC	4	29%	NO
6	(Malinka et al., 2022)	X	X	X	X	X	X	X					X	X		Banca	MB	RC	9	64%	SI
7	(Dawood et al., 2019)	X		X						X					X	Banca	CN	RC	4	29%	NO
8	(Salas et al., 2020)	X		X	X			X					X			Banca	ML	CO	5	36%	NO
9	(Fadlallah et al., 2020)	X	X	X			X	X					X			Banca	MB	CO	6	43%	SI
10	(Luo et al., 2020)	X		X	X			X		X					X	Banca	CN	RC	6	43%	SI
11	(Song et al., 2022)	X			X	X	X				X					Banca	MB	RC	5	36%	NO
12	(Ahmed et al., 2021)			X	X	X	X	X				X	X			Banca	MB	CO	7	50%	SI
13	(Mehrban et al., 2020)							X	X	X			X			Banca	MB	CO	4	29%	NO
14	(Kwon et al., 2019)	X						X		X					X	General	CN	RC	4	29%	NO
15	(Chen et al., 2021)	X		X	X			X		X			X			General	CN	RC	6	43%	SI
16	(Choi & Lee, 2018)			X				X		X			X		X	Banca	CN	RC	5	36%	NO
17	(Obaid et al., 2019)			X	X	X	X	X					X		X	Banca	CN	RI	7	50%	SI
18	(Tay & Mourad, 2020)	X		X	X			X	X	X			X			Banca	CN	RC	7	50%	SI
19	(Ileberi et al., 2021)	X		X		X		X		X			X		X	Banca	CN	CO	7	50%	SI
20	(Fan et al., 2018)	X		X	X	X	X	X	X				X		X	Banca	CN	RC	9	64%	SI
21	(Nasir et al., 2021)	X			X	X	X	X			X					General	MB	RI	6	43%	SI
22	(T. Jin et al., 2019)							X							X	Banca	CN	CO	2	14%	NO
23	(Huebner et al., 2019)						X	X	X						X	Banca	CN	RC	4	29%	NO
24	(Luz & Farias, 2020)	X		X	X	X	X	X	X		X		X			Banca	MB	RC	9	64%	SI
25	(Bambang & Priyatiningsih, 2020)	X		X				X	X						X	Banca	CN	RC	5	36%	NO
26	(Kurmanova et al., 2021)	X		X				X							X	Banca	CN	CO	4	29%	NO
27	(Cao, 2021)	X	X	X				X		X					X	Banca	MB	RC	6	43%	SI
28	(Wang et al., 2021)	X		X												Banca	ML	RI	2	14%	NO
29	(Chowdhury et al., 2022)	X		X				X	X		X				X	Banca	ML	RC	6	43%	SI
																Promedio Global			**5.45**		
																Porcentaje Global			**39%**		

Figura 9. Artículos factibles.

Entre los 29 artículos, sólo 14 artículos son factibles para su adopción y 15 no son factibles, es decir el 48% de artículos factibles para adopción e implementación y 52% no factibles, ver Fig. 10. En las características de NIS2: ML es Mercados en línea, MB es Motores de búsqueda, CN es Servicios de computación en la nube. De Problemas de NIS 2: RC es Resiliencia Cibernética, RI es Resiliencia Inconsistente, CO es bajo nivel de conciencia situacional. Entre el 48% de los artículos que son factibles, los servicios digitales de NIS 2: 7 son CN, 6 son MB y 1 es ML. Además, 4 son CO, 8 son RC, 2 son RI. Entre el 48% de los artículos que son factibles, la tecnología IA son factibles 5 artículos, en Blockchain son factibles 4 artículos, en Certificado son factibles 2 artículos, en Autenticación son factibles 10 artículos, en Monitoreo es factible 1 artículo, y en uso de Algoritmos son factibles 7 artículos.

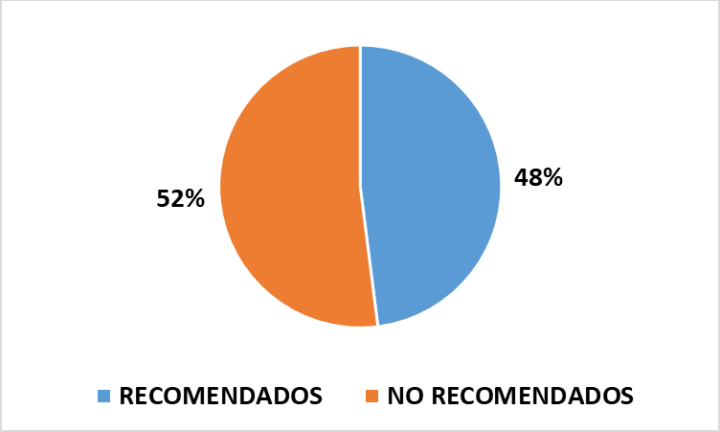


Figura 10. Aceptación de artículos.

Las propiedades como Tipo de Seguridad de Información, Características y Tecnologías en Seguridad de Información son cuantitativas, por ello es factible ver la distribución de todos los artículos, con valores de 28%, 40% y 32% respectivamente, ver Fig. 11.

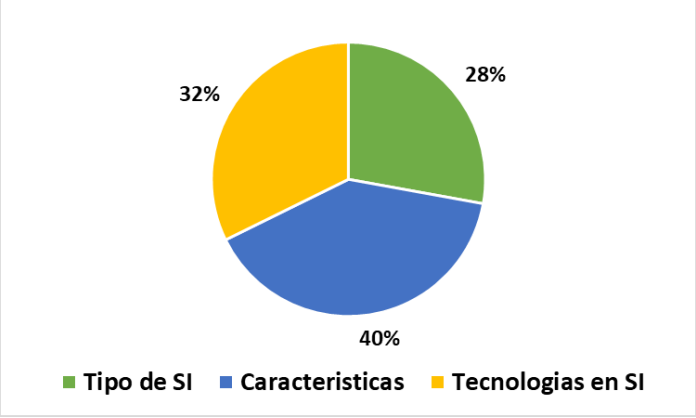


Figura 11. Distribución de características.

5. DISCUSIÓN

El 35% de los artículos factibles utilizan la Autenticación como medida de seguridad, sea por contraseña o biometría (huella o rostro o voz). El 17% de los artículos factibles utilizan algoritmos de Inteligencia Artificial, sea SVM, kNN, MLP, RF, Bayes, Machine Learning; IA se aplica para predecir el comportamiento de los usuarios y detectar posibles fraudes en las transacciones. El 14% de los artículos factibles utilizan la tecnología Blockchain para seguridad o integridad o privacidad de la información; Blokchain no solo brinda seguridad a la información, además vuelve inmutable las transacciones es decir no pueden ser cambiadas en el transcurso del tiempo. El 24% de los artículos factibles utilizan Algoritmos definidos por sus propias autorías para entregar nuevos o mejorados procesos de seguridad.

En esta investigación se desarrolló una revisión de literatura sistemáticamente y se verificó empíricamente con una escala detallada, sencilla y objetiva para evaluar la calidad de los artículos en el área de finanzas; los artículos obtenidos tienen una correlación positiva con las porcentajes medios de todos los artículos.

Esta investigación está limitada a artículos científicos relacionados con el área financiera y publicados en las bases de datos o bibliotecas científicas vinculadas a ciencias de computación o ingeniería de sistemas o áreas afines; los artículos comerciales o publicaciones en sitio web no científico no entran en esta investigación.

La pandemia generada por COVID-19 aceleró la transformación digital y sus riesgos en seguridad, por esta razón la seguridad en los sistemas de información aumentaron en la misma magnitud para proteger la información generada desde cualquier lugar.

En esta investigación se comparten nuestras observaciones sobre propuestas científicas de seguridades en el área financiera que pueden diferir de las seguridades que aplican los bancos ecuatorianos, además los bancos no publican ni comparten sus medidas de seguridad que aplican a los sistemas e información.

Como trabajo futuro se propone diseñar un modelo para asegurar la información en Blockchain, esta tecnología es utilizada en varias áreas y mantiene la información en forma encriptada e inmutable. Puede ser muy valioso generar una versión más amplia de esta investigación, estamos seguros que existen más tecnologías para asegurar los sistemas de información financiera especialmente para los usuarios finales.

6. CONCLUSIÓN

Los bancos comerciales adoptan y desarrollan nuevas tecnologías para asegurar las aplicaciones informáticas para todos sus clientes y proveedores, se utiliza Blockchain, IA, IoT, Big Data, entre otros, aunque la Transformación Digital conlleva nuevas amenazas, vulnerabilidades y riesgos en la seguridad de la información; la ciberdelincuencia es una complicación inmediata en la actualidad, y además las acciones que se tomen aseguran una economía segura en la sociedad bancarizada y el estado; los bancos están obligados a adoptar métodos y técnicas para afrontar cualquier riesgos en Seguridad de la Información y el tiempo de respuesta mínimo con posibles impactos mínimos en los servicios al mercado.

El mecanismo de autenticación es el más utilizado como modelos biométricos, patrones de comportamiento de las personas, lugares de acceso permitidos, entre otros; aunque en el mediano plazo las características biométricas deben ser actualizadas, la tendencia de los sistemas informáticos en el área financiera son aplicaciones móviles y esto implica nuevos riesgos como ubicación, redes públicas, perdida del dispositivo móvil, entre otros.

Las personas y cosas están cada vez más interconectadas porque la tecnología y tecnologías financieras permiten que las transacciones sean más sencillas, la *seguridad* es muy relevante, los investigadores, empresas privadas y consultores proporcionan soluciones seguras a las tecnologías financieras, además la seguridad y privacidad son importantes y relativas en esta investigación.

La Directiva NIS 2 mejora las características en ciberseguridad, orienta en forma estratégica y operativa a las áreas, servicios digitales y problemas específicos que se deben considerar en las seguridades de los sistemas de información.

REFERENCIAS

Ahmed, W., Rasool, A., & Javed, A. R. (2021). Security in Next Generation Mobile Payment Systems : A Comprehensive Survey. *IEEE Access*, *9*, 115932–115950. https://doi.org/10.1109/ACCESS.2021.3105450

Asamblea-Nacional-del-Ecuador. (2021). *Ley Organiza de Proteccion de Datos Personales*.

ASOBANCA. (2022). *Banca Privada Ecuatoriana*. https://asobanca.org.ec/wp-content/uploads/2022/06/Evolucion-de-la-Banca-05-2022-completo.pdf

Bambang Triantono, H., & Priyatiningsih, K. (2020). Fintech Accelerates Economic Recovery Solutions from Covid-19. *ACM International Conference Proceeding Series*, 25–28. https://doi.org/10.1145/3431656.3432053

Cao, L. (2021). AI in Finance: Challenges, Techniques and Opportunities. *SSRN Electronic Journal*, *55*(3). https://doi.org/10.2139/ssrn.3869625

Cárdenas Muñoz, J., Treviño Saldívar, E., Cuadrado Sánchez, G., & Ordoñez Parra, J. (2021). Análisis comparativo entre cooperativas de ahorro y crédito y bancos en el Ecuador. *Socialium*, *5*(2), 159–184. https://doi.org/10.26490/uncp.sl.2021.5.2.1000

Chen, Y. Y., Chen, C. T., Sang, C. Y., Yang, Y. C., & Huang, S. H. (2021). Adversarial attacks against reinforcement learning-based portfolio management strategy. *IEEE Access*, *9*, 50667–50685. https://doi.org/10.1109/ACCESS.2021.3068768

Choi, D., & Lee, Y. (2018). Eavesdropping of Magnetic Secure Transmission Signals and Its Security Implications for a Mobile Payment Protocol. *IEEE Access*, *6*, 42687–42701. https://doi.org/10.1109/ACCESS.2018.2859447

Chowdhury, O., Rishat, M. A. S. A., Azam, M. H. Bin, & Amin, M. Al. (2022). The Rise Of Blockchain Technology In Shariah Based Banking System. *ACM International Conference Proceeding Series*, 349–358. https://doi.org/10.1145/3542954.3543005

Dawood, E. A. E., Elfakhrany, E., & Maghraby, F. A. (2019). Improve profiling bank customer's behavior using machine learning. *IEEE Access*, *7*, 109320–109327. https://doi.org/10.1109/ACCESS.2019.2934644

Dumitrescu, B., Băltoiu, A., & Budulan, Ş. (2022). Anomaly Detection in Graphs of Bank Transactions for Anti Money Laundering Applications. *IEEE Access*, *10*, 47699–47714. https://doi.org/10.1109/ACCESS.2022.3170467

European Commission. (2020). Proposal for a directive on measures for a high common level of cybersecurity across the Union - NIS2. *COM (2020) 823 Final*, *0359*(2020/0359 (COD)), 108. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

Fadlallah, Y., Sbeiti, M., Hammoud, M., Nehme, M., & Fadlallah, A. (2020). On the Cyber Security of Lebanon: A Large Scale Empirical Study of Critical Vulnerabilities. *8th International Symposium on Digital Forensics and Security, ISDFS 2020*. https://doi.org/10.1109/ISDFS49300.2020.9116446

Fan, K., Li, H., Jiang, W., Xiao, C., & Yang, Y. (2018). Secure Authentication Protocol for Mobile Payment. *Tsinghua Science and Technology*, *23*(5), 610–620. https://doi.org/10.26599/TST.2018.9010031

Huebner, J., Schmid, C., Bouguerra, M., & Ilic, A. (2019). Finmars: A mobile app rating scale for finance apps. *ACM International Conference Proceeding Series*, 6–11. https://doi.org/10.1145/3357419.3357428

Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost. *IEEE Access*, *9*, 165286–165294. https://doi.org/10.1109/ACCESS.2021.3134330

Incel, O. D., Gunay, S., Akan, Y., Barlas, Y., Basar, O. E., Alptekin, G. I., & Isbilen, M. (2021). DAKOTA: Sensor and Touch Screen-Based Continuous Authentication on a Mobile Banking Application. *IEEE Access*, *9*, 38943–38960. https://doi.org/10.1109/ACCESS.2021.3063424

Jin, S. Y., & Xia, Y. (2022). CEV Framework: A Central Bank Digital Currency Evaluation and Verification Framework With a Focus on Consensus Algorithms and Operating Architectures. *IEEE Access*, *10*, 63698–63714. https://doi.org/10.1109/access.2022.3183092

Jin, T., Wang, Q., Xu, L., Pan, C., Dou, L., Qian, H., He, L., & Xie, T. (2019). FinExpert: Domain-specific test generation for FinTech systems. *ESEC/FSE 2019 - Proceedings of the 2019 27th ACM Joint Meeting European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 853–862. https://doi.org/10.1145/3338906.3340441

Kumar, R., Khan, A. I., Abushark, Y. B., Alam, M. M., Agrawal, A., & Khan, R. A. (2020). A Knowledge-Based Integrated System of Hesitant Fuzzy Set, AHP and TOPSIS for Evaluating Security-Durability of Web Applications. *IEEE Access*, *8*, 48870–48885. https://doi.org/10.1109/ACCESS.2020.2978038

Kurmanova, L., Nurdavliatova, E., Kurmanova, D., Galimova, G., & Khabibullin, R. (2021). Development of Digital Services and Information Security of Banks. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3487757.3490911

Kwon, H., Yoon, H., & Choi, D. (2019). Restricted Evasion Attack: Generation of Restricted-Area Adversarial Example. *IEEE Access*, *7*, 60908–60919. https://doi.org/10.1109/ACCESS.2019.2915971

Luo, G., Li, W., & Peng, Y. (2020). Overview of Intelligent Online Banking System Based on HERCULES Architecture. *IEEE Access*, *8*, 107685–107699. https://doi.org/10.1109/ACCESS.2020.2997079

Luz, M. A. Da, & Farias, K. (2020). The use of blockchain in financial area: A systematic mapping study. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3411564.3411579

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

Mehrban, S., Khan, M. A., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., Kiah, M. L. M., Abbas, F., & Hassan, M. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. *IEEE Access*, *8*, 23391–23406. https://doi.org/10.1109/ACCESS.2020.2970430

Naciones-Unidas. (2021). *Cybersecurity and the role of the Board of Directors in Latin America*. https://repositorio.cepal.org/bitstream/handle/11362/47655/1/S2100687_en.pdf

Nasir, A., Shaukat, K., Khan, K. I., Hameed, I. A., Alam, T. M., & Luo, S. (2021). What is Core and What Future Holds for Blockchain Technologies and Cryptocurrencies: A Bibliometric Analysis. *IEEE Access*, *9*, 989–1004. https://doi.org/10.1109/ACCESS.2020.3046931

Obaid, M., Bayram, Z., & Saleh, M. (2019). Instant Secure Mobile Payment Scheme. *IEEE Access*, *7*, 55669–55678. https://doi.org/10.1109/ACCESS.2019.2913430

Ramírez, K., & Mora, N. (2021). El Acoso Virtual y sus consecuencias en plataformas comunitarias, un mapeo sistemático. In *Universidad Politecnica Salesiana* (Vol. 1).

Salas, C. A. V., Prado, S. M. M., & Quiñonez, V. O. A. (2020). Is the Economic Growth of a Country Explained by the Banking System or the Capital Marketff the ARDL Model Applied in the Analysis for Ecuador. *ACM International Conference Proceeding Series*, 54–57. https://doi.org/10.1145/3409929.3414737

Song, Y., Sun, C., Peng, Y., Zeng, Y., & Sun, B. (2022). Research on Multidimensional Trust Evaluation Mechanism of FinTech Based on Blockchain. *IEEE Access*, *10*, 57025–57036. https://doi.org/10.1109/access.2022.3177275

Superintendecia_de_Bancos Ecuador. (2022). *Catastro Público SBE*. https://www.superbancos.gob.ec/bancos/catastro-publico/

Tay, B., & Mourad, A. (2020). Intelligent Performance-Aware Adaptation of Control Policies for Optimizing Banking Teller Process Using Machine Learning. *IEEE Access*, *8*, 153403–153412. https://doi.org/10.1109/ACCESS.2020.3015616

Wang, Q., Xu, L., Xiao, J., Guo, Q., Zhang, H., Dou, L., He, L., & Xie, T. (2021). FinFuzzer: One Step Further in Fuzzing Fintech Systems. *Proceedings - 2021 36th IEEE/ACM International Conference on Automated Software Engineering, ASE 2021*, 1111–1115. https://doi.org/10.1109/ASE51524.2021.9678675

Yildirim, N., & Varol, A. (2019). A research on security vulnerabilities in online and mobile banking systems. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 1–5. https://doi.org/10.1109/ISDFS.2019.8757495