



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado
Facultad de Ingeniería de Sistemas e Informática
Unidad de Posgrado

**Modelo Sectrabank para mitigar el fraude informático
en operaciones electrónicas a través de aplicaciones
bancarias en dispositivos Android**

TESIS

Para optar el Grado Académico de Doctor en Ingeniería de
Sistemas e Informática

AUTOR

Jhon Rigner MELENDEZ MELENDEZ

ASESOR

Dr. Jorge Victor MAYHUASCA GUERRA

Lima, Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Melendez, J. (2025). *Modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android*. [Tesis de doctorado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Jhon Rigner Melendez Melendez
Tipo de documento de identidad	DNI
Número de documento de identidad	42151848
URL de ORCID	https://orcid.org/0000-0003-3613-2569
Datos de asesor	
Nombres y apellidos	Jorge Victor Mayhuasca Guerra
Tipo de documento de identidad	DNI
Número de documento de identidad	07283032
URL de ORCID	https://orcid.org/0000-0002-6465-4738
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Rosa Sumactika Delgadillo Ávila
Tipo de documento	DNI
Número de documento de identidad	06445553
Miembro del jurado 1	
Nombres y apellidos	Igor Jovino Aguilar Alonso
Tipo de documento	DNI
Número de documento de identidad	32931485
Miembro del jurado 2	
Nombres y apellidos	Miguel Angel Cano Lengua
Tipo de documento	DNI
Número de documento de identidad	10324686
Datos de investigación	

Línea de investigación	Ciberseguridad
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Cercado de Lima Jr.Zorritos N° 1399 Latitud: -12.0491753 Longitud: -77.0570694
Año o rango de años en que se realizó la investigación	Setiembre 2022 – abril 2025
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Communication engineering and systems https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Vicedecanato de Investigación y Posgrado
Unidad de Posgrado

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE DOCTOR EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

A los veinte (20) días del mes de agosto de 2025, siendo las 11:30 am., se reunieron en el Auditorio Alfredo Celso Alva Bravo, el Jurado de Tesis conformado por los siguientes docentes:

Dra. Rosa Sumactika Delgadillo Ávila (Presidenta)
Dr. Igor Jovino Aguilar Alonso (Miembro)
Dr. Miguel Angel Cano Lengua (Miembro)
Dr. Jorge Victor Mayhuasca Guerra (Miembro Asesor)

Se inició la Sustentación invitando al candidato a Doctor **Jhon Rigner Melendez Melendez**, para que realice la exposición oral de la tesis para optar el Grado Académico de Doctor en Ingeniería de Sistemas e Informática, siendo la Tesis intitulada:

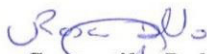
"Modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android".

Concluida la exposición, los miembros del Jurado de Tesis procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

..... QUINCE (15) BUENO

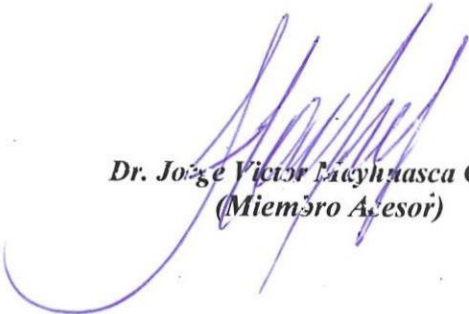
Por tanto, el presidente del Jurado, de acuerdo con el Reglamento General de Estudios de Posgrado, otorga al Magister **JHON RIGNER MELENDEZ MELENDEZ** el Grado Académico de Doctor en Ingeniería de Sistemas e Informática.

Siendo las 13:15 horas, el presidente del Jurado de Tesis, da por concluido el acto académico de Sustentación de Tesis.


Dra. Rosa Sumactika Delgadillo Ávila
(Presidenta)


Dr. Igor Jovino Aguilar Alonso
(Miembro)


Dr. Miguel Angel Cano Lengua
(Miembro)


Dr. Jorge Victor Mayhuasca Guerra
(Miembro Asesor)

CERTIFICADO DE SIMILITUD

Yo, JORGE VICTOR MAYHUASCA GUERRA en mi condición de asesor acreditado con Dictamen No 000051-2023-UPG-VDIP-FISI/UNMSM de la tesis, cuyo título es “Modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android”, presentado por el magíster Jhon Rigner Melendez Melendez para optar el grado de Doctor en Ingeniería de Sistemas e Informática.

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 4% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado/ título/ especialidad correspondiente.

Lima, 10 de Noviembre del 2024

Firma del Asesor

Nombres y Apellidos del asesor: Jorge Victor Mayhuasca Guerra
DNI 07283032

DEDICATORIA

A Dios, a mi querida madre Nina Yoli y mi padre Sumner Hernán, quienes con su ejemplo y sabiduría han guiado mi camino personal y profesional.

A la devoción personal y familiar por la Virgen de Guadalupe.

AGRADECIMIENTO

Agradezco a los catedráticos de la Universidad Nacional Mayor de San Marcos, por sus excelentes enseñanzas brindadas desde el inicio del doctorado hasta la culminación. Además, agradezco al Dr. Jorge Mayhuasca por haberme guiado en la línea de investigación, también agradezco a Paulo Calderón, Yordy Benites, David Morillo y Fabrizio Quijandria, estudiantes de Ingeniería de Software e Ingeniería Agroindustrial de la Universidad Nacional Mayor de San Marcos, quienes han aportado con su conocimiento en el desarrollo del modelo propuesto. Especialmente, agradezco a mis padres por apoyarme en mis estudios doctorales.

Ing. Jhon Rigner Meléndez Meléndez

Doctorando

ÍNDICE GENERAL

DEDICATORIA	iii
AGRADECIMIENTO	iv
ÍNDICE GENERAL	v
LISTA DE TABLAS	ix
LISTA DE FIGURAS	xi
RESUMEN	xiii
ABSTRACT	xiv
CAPÍTULO 1: INTRODUCCIÓN	1
1.1. Situación problemática	1
1.2. Formulación del problema	5
1.2.1. Problema general	5
1.2.2. Problemas específicos	5
1.3. Justificación de la investigación	6
1.3.1. Justificación teórica	7
1.3.2. Justificación práctica	7
1.4. Objetivos de la investigación	8
1.4.1. Objetivo general	8
1.4.2. Objetivos específicos	8
CAPÍTULO 2: MARCO TEÓRICO	9
2.1. Marco filosófico o epistemológico de la investigación	9
2.2. Antecedentes de investigación	10
2.2.1. Investigaciones relacionadas a los ataques de phishing y sus variantes	11
2.2.2. Secuestro y obtención del código OTP	14
2.2.3. Investigaciones relacionadas a los ataques de Fake App	15
2.2.4. Investigaciones relacionadas a los ataques de Sim Swapping	16
2.3. Bases teóricas	17

2.3.1.	Fundamentos teóricos de la seguridad digital	17
2.3.2.	Conceptos de la ciberseguridad y fraude digital	18
2.3.3.	Contexto actual de la ciberseguridad y el comportamiento cibercriminal	23
<i>CAPÍTULO 3: ESTADO DEL ARTE</i>		25
3.1.	Metodología para la revisión sistemática de la literatura.....	25
3.1.1.	Planificación de la revisión sistemática de la literatura	25
3.1.2.	Ejecución de la revisión sistemática de la literatura	29
3.1.3.	Resultados de la búsqueda de la revisión sistemática de la literatura	30
3.1.3.1.	Reporte de los estudios relacionados a los ataques de phishing	33
3.1.3.2.	Reporte de estudios relacionados a los ataques de Smishing	35
3.1.3.3.	Reporte de estudios relacionados a los ataques de Fake App	37
3.1.3.4.	Reporte de estudios relacionados a los ataques de SIM Swapping	39
3.1.3.5.	Reporte de estudios relacionados con modelos de seguridad biométrica.....	40
3.1.3.6.	Reporte de estudios relacionados con modelos de seguridad por código IMEI	43
3.1.3.7.	Reporte de estudios relacionados con modelos de seguridad por geolocalización.....	45
3.2.	Análisis y discusiones de la revisión sistemática de la literatura.	49
<i>CAPÍTULO 4: METODOLOGÍA PARA LA VALIDACIÓN DEL MODELO.....</i>		58
4.1.	Hipótesis.....	58
4.1.1.	Hipótesis general	58
4.1.2.	Hipótesis específicas	58
4.2.	Operacionalización de variables	58
4.3.	Matriz de consistencia	62
4.4.	Tipo y diseño de investigación	64
4.5.	Alcance del estudio	65
4.6.	Población y muestra	65
4.6.1.	Características de la población y muestra	65
4.6.2.	Tamaño de muestra	66

4.6.3.	Selección de muestra	67
4.7.	Desarrollo de la investigación	67
<i>CAPÍTULO 5: PROPUESTA DEL MODELO SECTRABANK</i>		69
5.1.	Fundamentos del Modelo Sectrabank.....	69
5.2.	Proceso del fraude	70
5.3.	Diseño del modelo Sectrabank.....	71
5.4.	Algoritmo de seguridad multicapa del modelo Sectrabank.....	72
5.5.	Código fuente del Modelo Sectrabank	74
5.5.1.	Habilitación de permisos.	74
5.5.2.	Huella digital.	75
5.5.3.	Ubicación.....	76
5.5.4.	IMEI.	77
5.5.5.	Mensaje OTP.	78
5.6.	Simulación de uso del Modelo Sectrabank.....	78
<i>CAPÍTULO 6: VALIDACIÓN, RESULTADOS Y DISCUSIÓN</i>		81
6.1.	Validación del modelo Sectrabank	81
6.1.1.	Selección de participantes	81
6.1.2.	Experimento	81
6.1.3.	Técnicas de recolección de datos	83
6.2.	Pruebas de hipótesis	84
6.2.1.	Prueba de normalidad	84
6.2.2.	Hipótesis general	85
6.2.3.	Hipótesis específica 1	87
6.2.4.	Hipótesis específica 2	88
6.2.5.	Hipótesis específica 3	90
6.2.6.	Hipótesis específica 4	91
6.3.	Análisis e interpretación de la información	92

a)	<i>Mitigación del fraude por Fake App.....</i>	93
b)	<i>Mitigación del fraude por SIM Swapping</i>	94
c)	<i>Percepción de accesibilidad, comprensión y facilidad de uso.....</i>	94
d)	<i>Aceptación del modelo: confiabilidad, eficacia y adaptabilidad</i>	95
6.4.	Análisis de resultados estadísticos.....	95
6.5.	Discusión de resultados	96
6.6.	Presentación de resultados	97
	<i>CAPÍTULO 7: CONCLUSIONES Y RECOMENDACIONES.....</i>	105
7.1.	Conclusiones.....	105
7.2.	Recomendaciones	106
	<i>REFERENCIAS BIBLIOGRÁFICAS.....</i>	109
	<i>ANEXOS.....</i>	125
	<i>Anexo 1: Glosario de términos</i>	125
	<i>Anexo 2: Estadística referente a cifras de Ciberseguridad en el mundo.....</i>	127
	<i>Anexo 3: Formulario para las personas que usaron el Modelo Sectrabank.....</i>	129
	<i>Anexo 4: Respuestas recopiladas en el formulario.....</i>	130
	<i>Anexo 5: Informe del grupo control y experimental con respecto a la usabilidad de parte de los usuarios.....</i>	132
	<i>Anexo 6: Artículo de Contribución de la Tesis.....</i>	142
	<i>Anexo 7 : Actas de validación de herramientas de recopilación de datos</i>	151
	<i>Anexo 8 : Imágenes de encuestas a la DIVINDAT</i>	164
	<i>Anexo 9: Constancia de cantidad de efectivos policiales encargados de investigar delitos informáticos</i>	166
	<i>Anexo 10: Constancia de cantidad de alumnos matriculados en decimo ciclo de ingeniería de software de la UNMSM.....</i>	167

LISTA DE TABLAS

Tabla 1 Cadena de fuentes de búsqueda para phishing y smishing	26
Tabla 2 Cadena de fuentes de búsqueda para Fake App y SIM Swapping.....	28
Tabla 3 Criterios de inclusión y exclusión.....	29
Tabla 4 Fuente de artículos seleccionados.....	30
Tabla 5 Ataques de Phishing con sus ventajas y limitaciones	33
Tabla 6 Ataques de Smishing con sus ventajas y limitaciones.....	36
Tabla 7 Ataques de Fake App con sus ventajas y limitaciones	38
Tabla 8 Ataques de SIM Swapping con sus ventajas y limitaciones.....	39
Tabla 9 Análisis comparativo de modelos biométricos	41
Tabla 10 Análisis comparativo de modelos por código IMEI	44
Tabla 11 Análisis comparativo de modelos por Geolocalización.....	46
Tabla 12 Operacionalización de la variable dependiente	60
Tabla 13 Operacionalización de la variable independiente	61
Tabla 14 Matriz de consistencia	62
Tabla 15 Prueba de normalidad	84
Tabla 16 Prueba Chi cuadrado hipótesis general.....	86
Tabla 17 Prueba Chi cuadrado hipótesis específica 1.....	87
Tabla 18 Prueba Chi cuadrado hipótesis específica 2.....	89
Tabla 19 Prueba Chi cuadrado hipótesis específica 3.....	90
Tabla 20 Prueba Chi cuadrado hipótesis específica 4.....	91
Tabla 21 Operaciones bancarias	98
Tabla 22 Frecuencia de respuestas sobre la efectividad del modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias.	99
Tabla 23 Gráfica sobre la percepción de mitigación del fraude informático en operaciones electrónicas mediante el modelo Sectrabank	100
Tabla 24 Frecuencia de respuestas sobre la efectividad del modelo Sectrabank para mitigar el fraude informático en la modalidad de Fake App.....	100
Tabla 25 Frecuencia de respuestas sobre la efectividad del modelo Sectrabank para mitigar el fraude informático en la modalidad de SIM Swapping	101
Tabla 26 Percepción de usabilidad del modelo Sectrabank.....	102

Tabla 27 Frecuencia respecto a la percepción de la confiabilidad del modelo Sectrabank	
.....	103

LISTA DE FIGURAS

Figura 1	Denuncias y pérdida monetaria mundial	1
Figura 2	Denuncias anuales en Perú	2
Figura 3	Denuncias por grupo generacional	2
Figura 4	Tipo de modalidades de ciberataque	3
Figura 5	Proceso de revisión de la literatura	30
Figura 6	Cantidad de artículos por base de datos	31
Figura 7	Cantidad de artículos por revista	32
Figura 8	Cantidad de artículos, libros y tesis	32
Figura 9	Estructura del proceso del fraude	70
Figura 10	Proceso de las capas de seguridad	72
Figura 11	Diagrama de flujo del Algoritmo de Seguridad Multicapa	74
Figura 12	Permisos necesarios para el desarrollo de la aplicación	75
Figura 13	Código de la Huella Digital	76
Figura 14	Código para obtener la ubicación	77
Figura 15	Código del IMEI	77
Figura 16	Código Mensaje OTP	78
Figura 17	Interfaces de usuario de la aplicación Sectrabank	79
Figura 18	Primera, Segunda y Tercera capa de seguridad	80
Figura 19	Operación final	80
Figura 20	Representación de la población	98
Figura 21	Gráfica de Operaciones bancarias	99
Figura 22	Gráfica sobre la percepción de mitigación del fraude informático en operaciones electrónicas mediante el modelo Sectrabank	100
Figura 23	Gráfica sobre la percepción de mitigación del fraude informático por Fake App	101
Figura 24	Gráfica sobre la percepción de mitigación del fraude informático mediante SIM Swapping	102
Figura 25	Gráfica de Percepción de usabilidad del modelo Sectrabank	103
Figura 26	Gráfica respecto a la percepción de la confiabilidad del modelo Sectrabank	104
Figura 27	Reporte de Ciberseguridad en América Latina y el Caribe	127

Figura 28 Estadísticas referentes a la vulnerabilidad de países a ciber ataques	127
Figura 29 Proyección del valor del mercado mundial de la ciberseguridad al 2023	128
Figura 30 Ingresos del mercado de la ciberseguridad en la región de Asia y el Pacífico desde 2017 hasta 2022, con previsiones hasta 2026	128
Figura 31 América es el mercado más grande entre las regiones seleccionadas en 2023	128

RESUMEN

El estudio desarrolla Sectrabank, un modelo de seguridad informática para mitigar el fraude en operaciones bancarias electrónicas en dispositivos Android. Aborda dos ataques frecuentes: SIM Swapping, que permite a ciberdelincuentes interceptar códigos de autenticación, y Fake Apps, que imitan aplicaciones oficiales para robar credenciales. Sectrabank refuerza la seguridad con un enfoque multicapa, combinando autenticación biométrica, validación de IMEI y geolocalización en tiempo real, ofreciendo una protección robusta y eficiente. Para evaluar la efectividad del modelo, se realizó un diseño experimental con dos grupos: un grupo experimental, donde los usuarios realizaron transacciones bancarias con la implementación de las medidas de seguridad del modelo Sectrabank y un grupo de control, sin medidas de seguridad. El modelo Sectrabank demostró ser una solución efectiva y confiable para mitigar el fraude en operaciones bancarias electrónicas en dispositivos Android, reduciendo significativamente los ataques de Fake Apps y SIM Swapping, con niveles de significación de 0.00 y altos porcentajes de efectividad en el grupo experimental (97.5% y 76.25%, respectivamente). Su diseño compacto y robusto, basado en un enfoque de seguridad multicapa que integra autenticación biométrica, validación del IMEI y geolocalización, permitió detectar y bloquear accesos fraudulentos antes de que se completaran transacciones no autorizadas. Además, los usuarios percibieron positivamente la usabilidad y confiabilidad del modelo, destacando su potencial para fortalecer la seguridad en plataformas bancarias móviles y su relevancia en un contexto de creciente fraude informático.

Palabras clave: Fake App; SIM Swapping; Cybercrime; Computer fraud; Mobile security; Authentication

ABSTRACT

The study develops Sectrabank, a cybersecurity model designed to mitigate fraud in electronic banking operations on Android devices. It addresses two common attacks: SIM Swapping, which allows cybercriminals to intercept authentication codes, and Fake Apps, which mimic official applications to steal credentials. Sectrabank enhances security through a multi-layered approach, combining biometric authentication, IMEI validation, and real-time geolocation, providing a robust and efficient protection mechanism. To evaluate the model's effectiveness, an experimental design was conducted with two groups: an experimental group, where users performed banking transactions with the security measures of the Sectrabank model, and a control group, without security measures. Sectrabank proved to be an effective and reliable solution for mitigating fraud in electronic banking operations on Android devices, significantly reducing Fake Apps and SIM Swapping attacks, with significance levels of 0.00 and high effectiveness rates in the experimental group (97.5% and 76.25%, respectively). Its compact and robust design, based on a multi-layered security approach integrating biometric authentication, IMEI validation, and geolocation, allowed for the detection and blocking of fraudulent access before unauthorized transactions were completed. Additionally, users perceived the model positively in terms of usability and reliability, highlighting its potential to enhance security in mobile banking platforms and its relevance in the context of increasing cyber fraud.

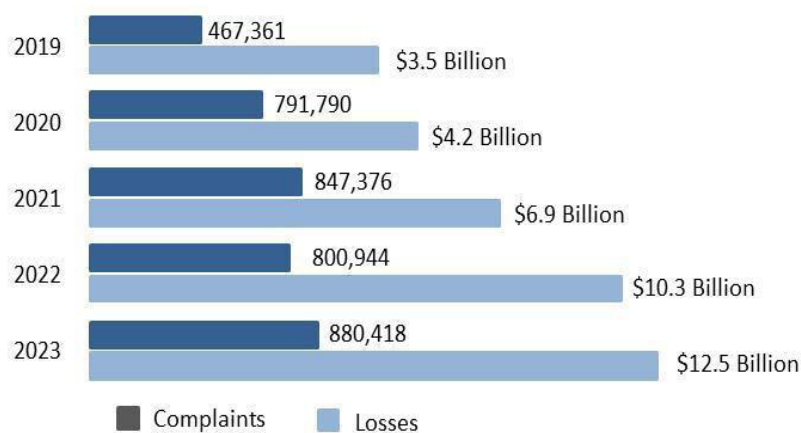
Keywords: Fake App; SIM Swapping; Cybercrime; Computer Fraud; Mobile Security; Authentication

CAPÍTULO 1: INTRODUCCIÓN

1.1. Situación problemática

Los ataques cibernéticos se incrementan cada año, con técnicas de ataques cada vez más sofisticados que son utilizados por los ciberdelincuentes con la finalidad de apoderarse del dinero de las cuentas bancarias de diferentes entidades. Este tipo de ataques provocan bloqueo de servicios, robo de información de los clientes, entre otros. En el año 2023, el FBI reportó el cibercrimen de los últimos cinco años, tal como ilustra la Figura 1, observándose el crecimiento en más del 300% en pérdidas de billones de dólares. Similar caso ocurre en Perú, como muestra la Figura 2, según los reportes de la “División de Investigación de Delitos de Alta Tecnología (DIVINDAT-Perú)” de la policía peruana, con el incremento del 300% en cinco años desde 2019, así como ocurren en diferentes países del mundo, Este fenómeno no es exclusivo de estos países, ya que se replica a nivel global, como se aprecia en el Anexo 2, titulado: *Estadísticas sobre Ciberseguridad en el Mundo*, que presenta datos relevantes en las Figuras 27, 28, 29 y 30.

Figura 1
Denuncias y pérdida monetaria mundial



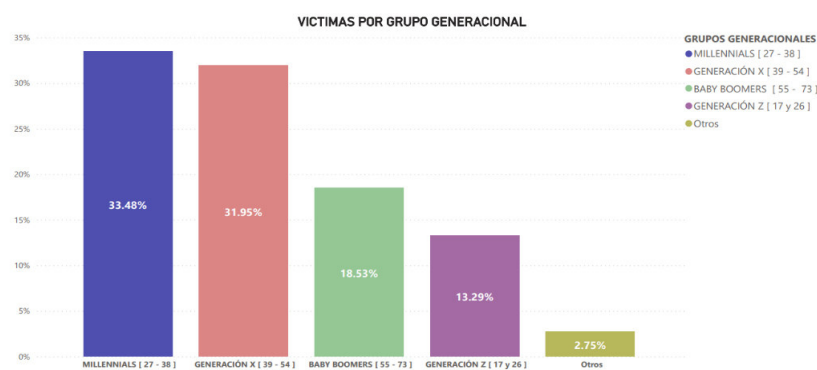
Nota. Pérdida en billones de dólares y la cantidad de denuncias recibidas por el FBI entre los años 2019 y 2023. Obtenido de FBI Releases Internet Crime Report (p.7) por Federal Bureau of Investigation, 2024.

Figura 2
Denuncias anuales en Perú



Nota. El presente histograma refleja la cantidad de denuncias anuales registradas en el Perú, por la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), donde se ha realizado un análisis de víctimas de acuerdo al grupo generacional (Figura 3).

Figura 3
Denuncias por grupo generacional

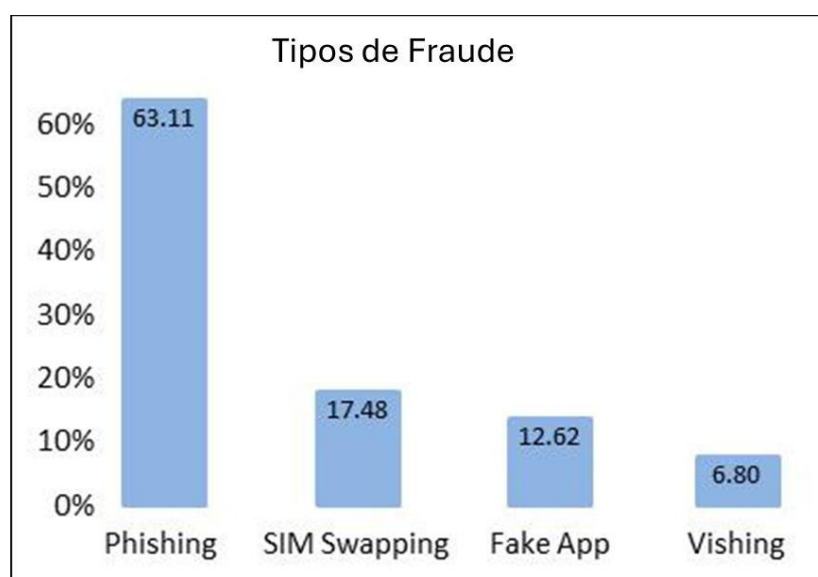


Nota. El presente histograma refleja la cantidad de denuncias por grupo generacional en Perú

La información proporcionada por la DIVINDAT-Perú, incluye, también, los porcentajes de tipos de modalidades usadas en los ciberataques, donde el 63.11% de las 18,830 denuncias registradas en el año 2023 (Figura 4), han sido por la modalidad de Phishing y el 17.48% por la modalidad de SIM Swapping y el 12.62% por la modalidad de

Fake App y en su menor porcentaje la modalidad de Vishing con un 6.80%. Es preciso mencionar que aleatoriamente se ha revisado el contenido de algunas denuncias y se ha obtenido información que algunos casos denunciados por Smishing han sido registrados como phishing, ello sucede porque algunos funcionarios policiales no se familiarizan con los términos ciberdelictivos, más aún si se tiene en consideración que las denuncias han sido obtenidas de diferentes dependencias policiales a nivel nacional.

Figura 4
Tipo de modalidades de ciberataque



Nota. El presente histograma presenta las modalidades de ciberataque más empleadas en Perú

En la era digital, el fraude informático ha evolucionado de manera alarmante, afectando directamente las operaciones bancarias en línea y poniendo en riesgo la seguridad financiera de los usuarios. Específicamente, fraudes como el SIM Swapping y las Fake Apps han demostrado ser altamente efectivos para comprometer la identidad digital y obtener acceso no autorizado a cuentas bancarias. Estos ataques han crecido exponencialmente con la masificación de dispositivos móviles y la digitalización de los servicios financieros (Ekeh et al., 2022).

A nivel mundial, el impacto económico del fraude informático es devastador. La pérdida anual global por fraude informático se estima en miles de millones de dólares, con

algunas cifras que señalan que el costo anual en los EE. UU, supera los 400 mil millones de dólares. Además, el Internet Crime Complaint Center (IC3) reportó 467,361 quejas de delitos de fraude informático en línea en los EE. UU., con pérdidas superiores a 3.5 mil millones de dólares en un solo año (Hilal et al. 2022). En particular, el SIM Swapping, un método en el que los atacantes logran obtener el control de la tarjeta SIM de la víctima para interceptar sus códigos de autenticación, representa una de las amenazas más críticas contra la seguridad bancaria (Ekeh et al., 2022). Por otro lado, las Fake Apps, aplicaciones maliciosas que imitan el diseño y la funcionalidad de aplicaciones bancarias reales, generan riesgos de seguridad y privacidad de la información que enfrentan las aplicaciones de banca móvil y pagos (Bassolé et al., 2020)

La comunidad académica y el sector financiero han desarrollado diversas estrategias para mitigar estos ataques. Enfoques tradicionales incluyen la autenticación en dos pasos (OTP), el monitoreo de transacciones sospechosas y el bloqueo de cuentas por actividad inusual. Sin embargo, estas medidas han demostrado ser insuficientes, ya que el SIM Swapping permite interceptar OTPs y las Fake Apps evaden mecanismos de detección (Bello y Olufemi, 2024).

Para mejorar la seguridad, se han implementado modelos basados en inteligencia artificial (IA) y aprendizaje automático, que permiten detectar patrones de fraude en tiempo real. Diferentes modelos de machine learning han sido utilizados para mejorar la detección de fraudes en transacciones financieras, aumentando la precisión de los sistemas de prevención (Alatawi, M. N., 2025). Sin embargo, muchas de estas soluciones dependen de datos históricos y no previenen ataques en el momento en que ocurren, dejando a los usuarios vulnerables (Brown et al., 2024)

Dada la creciente sofisticación de los ataques informáticos, es fundamental implementar un modelo que no solo detecte fraudes, sino que además prevenga de forma activa el acceso no autorizado a cuentas bancarias, con especial atención a los usuarios del sistema operativo Android, el cual, según Statcounter Global Stats (2024), concentra aproximadamente el 72 % del uso global de dispositivos móviles, lo que lo convierte en el principal objetivo de los ciberdelincuentes. En este contexto, el modelo Sectrabank se presenta como una solución innovadora al integrar en un mismo esquema la autenticación

biométrica, la verificación del IMEI y la validación mediante geolocalización. Esta combinación de factores de seguridad permite mitigar de manera efectiva el fraude informático, reduciendo significativamente las posibilidades de que los atacantes logren apropiarse de las claves OTP y comprometan las transacciones electrónicas. Como parte de los aportes preliminares de esta investigación, se publicó el artículo titulado “*Modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android*” en la *Revista Peruana de Computación y Sistemas*, volumen 6(2), páginas 3-13, año 2024 de la UNMSM. Esta publicación, disponible en <https://doi.org/10.15381/rpcs.v6i2.29031>, recoge los fundamentos iniciales del modelo propuesto, validando su relevancia tanto académica como práctica. Dicha contribución se encuentra referenciada en el Anexo 6, titulado: *Artículo de Contribución de la Tesis*.

1.2. Formulación del problema

1.2.1. Problema general

¿Es posible desarrollar un modelo denominado Sectrabank que permita mitigar efectivamente el fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android, mejorando la detección de Fake App y SIM Swapping, así como la aceptación y usabilidad percibida por los usuarios?

1.2.2. Problemas específicos

- a. ¿Cómo debe desarrollarse un modelo denominado Sectrabank que permita la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android?
- b. ¿Qué mecanismos deben integrarse en el desarrollo del modelo Sectrabank para mitigar el fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android?
- c. ¿Qué características deben ser consideradas en el desarrollo del modelo Sectrabank para garantizar que sea percibido adecuadamente en términos de accesibilidad, comprensión y facilidad de uso por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android?

- d. ¿Qué criterios deben ser contemplados en el desarrollo del modelo Sectrabank para validar la aceptación por parte de los usuarios en términos de confiabilidad, eficacia y adaptabilidad en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android?

1.3. Justificación de la investigación

La tesis sobre el "Modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android" es crucial en el contexto actual debido a la creciente amenaza de los delitos informáticos en el entorno financiero. Este modelo no solo busca proteger los activos financieros de individuos y empresas, sino que también promueve la confianza y estabilidad en el sistema financiero, empodera a los usuarios con medidas de seguridad adicionales, impulsa la innovación tecnológica en ciberseguridad y tiene el potencial de transformar la industria bancaria al fortalecer relaciones con los clientes y cumplir con regulaciones de seguridad más estrictas.

En el ámbito de la ciberseguridad financiera, el Phishing ha sido identificado como la modalidad de ataque con mayor incidencia, representando el 63.11% de los fraudes informáticos en operaciones bancarias. Sin embargo, la industria ha desarrollado múltiples estrategias para su mitigación, incluyendo filtros anti-phishing en correos electrónicos, autenticación multifactor (MFA) y campañas de concientización (West, Bhattacharya y Islam, 2015). En contraste, los ataques de Fake App y SIM Swapping presentan desafíos más complejos que comprometen la privacidad y la confidencialidad, vulnerando los permisos de acceso y el código de aplicaciones bancarias (Bassolé et al., 2020). Además, los sistemas de seguridad convencionales han resultado insuficientes para la identificación temprana de estos fraudes, ya que los ciberdelincuentes logran falsificar la identidad auténtica del usuario como contraseñas y códigos de verificación OTP (Alzomai, M.H. 2011). Estudios recientes han demostrado que la implementación de modelos avanzados basados en autenticación biométrica, verificación de IMEI y geolocalización es una estrategia efectiva para la prevención activa de estos ataques (Alatawi, M. N. 2025). Por esta razón, el presente estudio se enfoca en diseñar e implementar el modelo Sectrabank,

una solución integral que aborda de manera específica los fraudes de Fake App y SIM Swapping, mitigando vulnerabilidades críticas en la seguridad bancaria móvil.

1.3.1. Justificación teórica

La justificación teórica de esta tesis se fundamenta en la necesidad de abordar el creciente problema de los delitos informáticos, especialmente en el contexto de las operaciones bancarias electrónicas a través de dispositivos Android. La literatura existente sobre ciberseguridad y fraude informático proporciona un marco teórico sólido que respalda la importancia de desarrollar estrategias y modelos específicos para mitigar estos riesgos. Además, el estudio de modelos previos y teorías relacionadas con la seguridad informática en el sector bancario brinda insights valiosos para diseñar y evaluar el modelo Sectrabank propuesto.

1.3.2. Justificación práctica

En términos prácticos, esta investigación tiene como objetivo proporcionar una solución efectiva y aplicable para las instituciones bancarias que enfrentan amenazas constantes de fraude informático en sus plataformas móviles. Los ciberdelincuentes, mediante técnicas de ingeniería social como phishing, smishing o vishing, obtienen información confidencial de las cuentas bancarias de sus víctimas. Posteriormente, emplean estrategias como Fake App y SIM Swapping para acceder o interceptar códigos de autenticación, como claves OTP o tokens, con el propósito de sustraer fondos ilícitamente. Ante este panorama, se propone el modelo Sectrabank, diseñado específicamente para mitigar estos ataques, evitando que los ciberdelincuentes se apoderen de las credenciales críticas que permiten la ejecución de transacciones fraudulentas.

La implementación efectiva del modelo Sectrabank podría contribuir significativamente a reducir la incidencia de fraudes y proteger los activos financieros de los clientes. Además, esta investigación proporcionará pautas prácticas para la gestión de la seguridad informática en el sector bancario, ayudando a las organizaciones a fortalecer sus medidas de protección y respuesta ante amenazas cibernéticas.

La metodología de esta tesis se basa en un enfoque mixto que combina métodos cualitativos y cuantitativos. Se realizará un análisis exhaustivo de la literatura existente

para identificar las mejores prácticas y los modelos relevantes en el campo de la seguridad informática y la banca electrónica. Además, se llevarán a cabo estudios de caso y entrevistas con expertos en ciberseguridad y representantes de la Policía encargados de investigar Delitos Informáticos, para validar y refinar el modelo propuesto. Este enfoque metodológico integral permitirá una comprensión completa de los desafíos y oportunidades asociados con la implementación del modelo Sectrabank.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Desarrollar el modelo Sectrabank para mitigar efectivamente el fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android, mejorando la detección de Fake App y SIM Swapping, así como la aceptación y usabilidad percibida por los usuarios

1.4.2. Objetivos específicos

- a.** Desarrollar un modelo denominado Sectrabank que permita la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.
- b.** Integrar mecanismos funcionales y tecnológicos en el modelo Sectrabank que permitan mitigar el fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.
- c.** Incorporar características de accesibilidad, comprensión y facilidad de uso en el modelo Sectrabank, considerando las necesidades de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.
- d.** Establecer criterios de confiabilidad, eficacia y adaptabilidad en el desarrollo del modelo Sectrabank que favorezcan su aceptación por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

CAPÍTULO 2: MARCO TEÓRICO

2.1. Marco filosófico o epistemológico de la investigación

El fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android, ha sido un tema de creciente interés en los últimos años, debido a la constante evolución de las amenazas cibernéticas y la creciente dependencia de los usuarios en los servicios financieros digitales. Diversos estudios han abordado las vulnerabilidades existentes en estas aplicaciones, así como las estrategias necesarias para mitigar los riesgos asociados. Chen et al. (2020) realizaron un análisis empírico sobre los riesgos de seguridad en aplicaciones bancarias Android, identificando fallas críticas que han sido explotadas por ciberdelincuentes para comprometer la integridad de las transacciones. Su estudio resalta la falta de protocolos de cifrado adecuados en muchas aplicaciones bancarias, lo que permite ataques de intermediario (MITM) y la interceptación de datos sensibles. En esta misma línea, Ulqinaku et al. (2019) señalaron que la función “Scan-and-Pay”, ampliamente utilizada en diversas plataformas bancarias, presenta riesgos significativos al permitir la manipulación de códigos QR para redirigir pagos a cuentas fraudulentas sin que los usuarios se percaten del engaño. Este hallazgo es relevante, ya que demuestra cómo las innovaciones en pagos digitales pueden convertirse en vectores de ataque cuando no se implementan con medidas de seguridad robustas.

Asimismo; Zambrano y Suárez (2020) enfatizaron la problemática de los dispositivos sin soporte oficial, que muchas veces no reciben actualizaciones de seguridad, exponiendo a los usuarios a malware bancario y vulnerabilidades persistentes que no pueden ser corregidas sin la intervención del fabricante. Esta situación afecta especialmente a usuarios con dispositivos de gama baja o modelos más antiguos, quienes, por limitaciones económicas, continúan utilizando equipos sin protección adecuada. Frente a estas amenazas, Abi Din et al. (2021) propusieron la implementación de sistemas antifraude éticos que puedan identificar y bloquear actividades sospechosas sin afectar la experiencia del usuario, promoviendo así un equilibrio entre seguridad y usabilidad. En este sentido, Sharma y Ghosh (2021) desarrollaron un protocolo de autenticación ligero y seguro para pagos móviles, el cual emplea múltiples factores de verificación sin comprometer la velocidad ni la accesibilidad de las transacciones, abordando una de las

principales preocupaciones en la banca digital: la necesidad de implementar medidas de seguridad sin generar fricción en la experiencia del cliente.

Desde un enfoque más técnico, (Bassolé et al., 2020), analizan las vulnerabilidades de aplicaciones de banca móvil y pagos en Android, destacando riesgos de privacidad y seguridad. Se identifican fallos en la gestión de credenciales y almacenamiento de datos sensibles que facilitan ataques como phishing e inyección de código, (Kuttiyappan y Rajasekar, 2023) exploraron el uso de técnicas de aprendizaje profundo para detectar ataques maliciosos en sistemas bancarios, destacando la importancia de la inteligencia artificial en la detección de fraudes financieros en tiempo real. Su estudio demostró que los modelos de machine learning pueden identificar patrones sospechosos en transacciones electrónicas, permitiendo a las instituciones financieras reaccionar de manera inmediata ante posibles amenazas.

2.2. Antecedentes de investigación

La mayoría de las investigaciones sobre el fraude informático, se centran en la detección de phishing y sus variantes utilizando algoritmos de inteligencia artificial. Sin embargo, hay pocos estudios que abordan técnicas de mitigación para prevenir la consumación de estos ataques. Esta brecha en la investigación es preocupante, debido a que las pérdidas a nivel mundial ascienden a miles de millones de dólares, pérdidas económicas que se incrementan continuamente. En efecto, varios estudios de investigación se centran en la detección de phishing en URLs y contenido de páginas web, así como en mensajes SMS y correos electrónicos, utilizando técnicas y algoritmos de aprendizaje automático (ML) y aprendizaje profundo (DL) (Su y Su, 2023). Entre las técnicas más utilizadas se encuentran las redes neuronales artificiales (ANN), las redes neuronales convolucionales (CNN), las redes neuronales recurrentes (RNN), los algoritmos genéticos (GA), los bosques aleatorios (RF), la memoria a largo plazo (LSTM), las unidades recurrentes con compuerta (GRU), las representaciones de codificador bidireccional de transformadores (BERT), y las metaheurísticas como la optimización de algas artificiales (AAO) y la optimización de malezas invasoras (IWO). Estas técnicas han alcanzado precisiones que van desde el 87% hasta el 99.8% (Mongay Batalla., 2024).

2.2.1. Investigaciones relacionadas a los ataques de phishing y sus variantes

En la fase inicial de los ataques de fraude informático, los ciberdelincuentes emplean técnicas como el phishing, smishing y vishing para engañar a las víctimas y obtener sus datos bancarios. Estas técnicas involucran el uso de correos electrónicos fraudulentos, mensajes de texto y llamadas telefónicas falsas que aparentan ser de instituciones legítimas, con el fin de obtener información sensible como contraseñas, información de las tarjetas bancarias y línea telefónica afiliada.

Para contrarrestar esta amenaza, varios estudios de investigación se centran en la detección de phishing en URLs y contenido de páginas web, así como en mensajes SMS y correos electrónicos, utilizando técnicas y algoritmos de aprendizaje automático (ML) y aprendizaje profundo (DL). Entre las más utilizadas se encuentran las redes neuronales artificiales (ANN), las redes neuronales convolucionales (CNN), las redes neuronales recurrentes (RNN), los algoritmos genéticos (GA), los bosques aleatorios (RF), la memoria a largo y corto plazo (LSTM), las unidades recurrentes con compuertas (GRU), las representaciones de codificadores bidireccionales de transformadores (BERT) y las metaheurísticas como la optimización de algas artificiales (AAO) y la optimización de malas hierbas invasoras (IWO). Estas técnicas han alcanzado precisiones que oscilan entre el 87% y el 99.8% (Mongay Batalla, 2024; Su & Su, 2023).

En la detección de phishing en URLs, el modelo basado en CNN identifica caracteres y alcanza una precisión del 98.8%, entrenado con 318,642 URLs (Aljofey et al., 2020). En esa línea, se propone un modelo híbrido de CNN y RNN-LSTM con una precisión del 99.01% (Shaiba et al., 2022). Modelos como RNN-LSTM, junto con Bi-LSTM y GRU, logran una precisión de hasta el 99% (Roy et al., 2022). Por otra parte, otro enfoque emplea LSTM-CNN para la detección de phishing en páginas web, alcanzando una precisión del 99.2% con 20,000 URLs (Alshingiti et al., 2023). Asimismo, otras propuestas formulan un modelo basado en CNN con atributos BERT, obteniendo una precisión del 96.66% en URLs de phishing de Kaggle (Elsadig et al., 2022). De igual forma, se utilizan los mismos datos de Kaggle para un modelo óptimo de red autoencoder profunda (ODAE-WPDC), combinando DL con las metaheurísticas AAO e IWO, logrando una precisión del 99.28% (Alqahtani et al., 2022).

En otro estudio, se aplica el método de interpolación de reglas difusas (FRI-Incircle), alcanzando una efectividad del 97.58% en la detección de URLs de phishing (Almseidin et al., 2022). Bu y Kim (2022) combinan CNN con GA para optimizar la selección de características, mejorando el recall. Finalmente, los algoritmos de RF son empleados para la detección de URLs de phishing, logrando precisiones del 97.98%, 97.5% y 98.5%, respectivamente (Sahingoz et al., 2019; Alani & Tawfik, 2022; Ahmed et al., 2022).

El grupo de Sahingoz et al. (2019) extrajo atributos utilizando procesamiento de lenguaje natural (NLP) en el texto de las URLs, mientras que Alani y Tawfik (2022) consideraron RF en el sistema PhishNot, entrenado con 57,024 URLs, de las cuales 18,062 son de phishing. Otro enfoque, SPWalk, basado en ML supervisado, alcanza una precisión del 95% (Liu & Fu, 2020).

En el análisis de sitios web de phishing, predominan las técnicas de aprendizaje automático (ML). Por ejemplo, se utiliza Random Forest (RF) para clasificar sitios web como benignos, spam o maliciosos, logrando una precisión del 98.38%. Este análisis incluye características léxicas de las URLs, direcciones IP, longitud, caracteres sospechosos, prefijos y sufijos, basado en una muestra de 3,000 URLs (Sathya et al., 2020). De manera similar, se aplican técnicas de ML en el modelo PhishHaven para detectar phishing generado tanto por IA como por humanos en 100,000 URLs, logrando una precisión del 98% (Sameen et al., 2020). Otro enfoque alcanza una precisión del 98.90% utilizando un modelo ML multicapa en el análisis de conjuntos de sitios web (Kalabarige et al., 2022).

El análisis de ataques de homógrafos en sitios web combina la función hash y RF, logrando una precisión del 99.8% (Almuhaideb et al., 2022), mientras que otra investigación, utilizando heurísticas y web crawling, alcanza una precisión del 95.18% (Mohamed et al., 2022). En este contexto, se utilizan métodos de aprendizaje continuo, como Learning without Forgetting (LWF) y Elastic Weight Consolidation (EWC), en una red neuronal preentrenada para la detección de phishing en datos de 170,000 páginas

recolectadas en los años 2018-2020. Este modelo puede adaptarse al comportamiento de nuevas técnicas de ataque (Ejaz et al., 2023).

La suplantación de logotipos de sitios web se analiza mediante procesamiento de imágenes y RF, logrando una precisión del 87% (Panda et al., 2022). Otro enfoque, Combined Correlation Features Selection (CCrFS), detecta sitios web de phishing utilizando ML con una precisión del 97.07% (Moedjahedy et al., 2022).

En otro estudio, se detecta phishing en tiempo real con una precisión, recall y F1 score del 99% utilizando el modelo Phish Transformer, un CNN-transformer para clasificación, con datos extraídos de URLs de sitios web (Asiri & Al-Ghamdi, 2023). En cuanto al smishing, la detección implica analizar señales de phishing en elementos relacionados con textos recibidos vía SMS y correos electrónicos. En esta categoría, se propone un modelo anti-smishing basado en algoritmos de correlación y aprendizaje automático, logrando una precisión del 98.4% (Sonowal, 2020).

Otro estudio analiza SMS móviles inspeccionando el comportamiento de las URLs, el código fuente de los sitios web vinculados y la descarga de archivos APK maliciosos, logrando una precisión del 96.29% (Mishra & Soni, 2020). Otro enfoque detecta y previene el spam SMS utilizando RIPPER y C4.5 con una precisión del 98.08% (Akande et al., 2023). Otro modelo híbrido de CNN y LSTM se aplica para la detección de spam en SMS con una precisión del 98.38% (Ghourabi et al., 2020). Finalmente, el clasificador ExtraTree RF es un modelo híbrido dirigido a usuarios de dinero móvil, detectando y previniendo mensajes infectados en tiempo real con una precisión del 99.8% (Mambina et al., 2022).

El smishing-email se aborda mediante un algoritmo de selección de características de búsqueda binaria (BSFS), el cual fue entrenado en 3,428 correos electrónicos con diversos atributos extraídos, logrando una precisión del 97.41% (Sonowal, 2020). Un modelo de machine learning XGBoost junto con LNP para la extracción de atributos y técnicas de agrupación temática alcanza un F1 score del 99.95% en 6,429 correos electrónicos (Gualberto et al., 2020).

Otro enfoque basado en SGBost combina atributos de texto, datos de URLs e imágenes, logrando una precisión del 94% (Shaukat et al., 2023). El análisis de palabras y

palabras contaminadas en correos electrónicos, mediante algoritmos LSTM y CNN, resulta en una precisión del 99.81% y un F1 score del 99.74% (Stevanović, 2022). Asimismo, la técnica de agrupación Mean Shift DBSCAN se emplea para clasificar correos electrónicos de phishing según su origen y URLs relativamente homogéneas (Althobaiti et al., 2023). El algoritmo FMMPED, diseñado para la detección de correos electrónicos de phishing, logra una precisión del 97.97% (Qi et al., 2023).

En el caso del vishing, el método de atención ID CNN-BiLSTM combina enfoques centrados en datos y modelos de IA para la detección de discursos en coreano, mostrando un rendimiento notable (Boussougou & Park, 2023). El método de fuerza bruta, empleado por ciberdelincuentes para infiltrarse en sistemas informáticos, implica múltiples intentos de inicio de sesión con diversas combinaciones de contraseñas, mediante pruebas exhaustivas ejecutadas por programas diseñados para descifrar contraseñas encriptadas usando algoritmos específicos (Giffary & Ramadhani, 2022; Brăslășu et al., 2023). A pesar del avance en la detección de phishing, smishing y vishing utilizando técnicas de IA, es crucial un enfoque más holístico que considere las limitaciones de estas técnicas y explore soluciones complementarias. Por ejemplo, la dependencia excesiva en el análisis de URLs y contenido puede ser vulnerable a técnicas de ofuscación y ataques de día cero. Además, la detección de smishing y vishing requiere una comprensión más profunda del contexto y la semántica del lenguaje utilizado por los atacantes, lo que representa un desafío para los algoritmos actuales. Es necesario investigar nuevas estrategias que combinen el análisis de datos con la comprensión del comportamiento humano y el contexto social, con el fin de desarrollar mecanismos de defensa más robustos y efectivos contra el fraude cibernético. Asimismo, se debe fomentar la investigación en técnicas de mitigación proactiva, que busquen prevenir la consumación de los ataques en lugar de simplemente detectarlos.

2.2.2. Secuestro y obtención del código OTP

Los ciberdelincuentes, tras obtener información sensible como contraseñas, información de las tarjetas bancarias y línea telefónica afiliada, buscan acceder a la contraseña de un solo uso (OTP) que los usuarios reciben en sus dispositivos móviles. Este código, de corta duración y generación automática, es crucial para autorizar transacciones financieras. Para interceptar dicho código, los atacantes utilizan técnicas como Fake Apps

y SIM Swapping. En el Fake Apps, los ciberdelincuentes engañan a las víctimas mediante falsas ofertas de préstamos o promociones atractivas, persuadiéndolas para que instalen aplicaciones maliciosas. Estas aplicaciones permiten el acceso total al dispositivo móvil, facilitando el control remoto de las apps bancarias instaladas y permitiendo la ejecución de transacciones fraudulentas hacia cuentas de terceros, conocidas como "cuentas mulas". Por otro lado, en el caso de SIM Swapping, los delincuentes toman el control de la línea telefónica de la víctima al duplicar la tarjeta SIM, lo que les permite interceptar los códigos OTP y recuperar contraseñas bancarias. Sin embargo, existen pocos trabajos relacionados con la mitigación de ataques de Fake App y SIM Swapping entre los que se destacan los siguientes:

2.2.3. Investigaciones relacionadas a los ataques de Fake App

Según los estudios en la categoría de Fake Apps, los cibercriminales suplantando las aplicaciones más populares para engañar y manipular el contenido sensible del usuario, ejecutándose en segundo plano sin ser detectadas (Arunakumari et al., 2022). Anteriormente, se investigaron 150,000 muestras de aplicaciones populares, determinando mediciones cuantitativas y características de las aplicaciones falsas, así como las tendencias y estrategias evasivas utilizadas en su programación (Tang et al., 2019). De manera similar, un estudio sobre más de 6 millones de aplicaciones Android reveló una mayor prevalencia de aplicaciones maliciosas, falsas y clonadas en plataformas de comercio chino (Wang et al., 2018). Otro análisis de más de 1,500 dominios de estafa y 300 aplicaciones falsas detectó 94 familias de dominios fraudulentos y 30 familias de aplicaciones falsas, causando pérdidas superiores a medio millón de dólares (Xia et al., 2020). En esta categoría, existen varios trabajos de detección, como uno que aborda TrickBot, un malware de Fake App, utilizando RF con una precisión del 99.95% y una tasa de detección verdadera del 91.7% (Gezer et al., 2019). El método MSimDroid, basado en TLSH y MinHash, detecta aplicaciones IoT falsas con una precisión superior al 99% (Wu et al., 2020). Se ha propuesto también un modelo ANUBIS, basado en BNN, para detectar amenazas persistentes avanzadas (APT) utilizando gráficos de procedencia, logrando una precisión superior al 99% (Anjum et al., 2022). Otro enfoque utiliza la infraestructura de la red móvil y las API de comunicación móvil para verificar la compatibilidad entre los números de teléfono

registrados y los utilizados en los dispositivos, mostrando un 100% de efectividad en sus escenarios de prueba (Prayogi y Aji, 2023). Una vez detectadas las aplicaciones en un teléfono clonado, la mitigación es inmediata. Los trabajos relacionados dirigen esfuerzos hacia la detección, como el que formulan un método híbrido de grafo de flujo de control (CFG) y RNN con alta capacidad para detectar aplicaciones clonadas en sistemas sociales IoT 5G (Ullah et al., 2021). Un modelo basado en el "árbol de diseño fusionado" (MLT) es también eficiente en la detección de clones en grandes conjuntos de datos y la mitigación de ciberataques (Xie et al., 2021). Se amplía este enfoque utilizando aprendizaje profundo basado en el árbol de sintaxis abstracta (AST), logrando alta eficiencia (Ullah et al., 2020; Arslan, 2021). Otro análisis empleó un algoritmo de análisis estático para detectar aplicaciones reempaquetadas en Google Play, revelando vulnerabilidades que permiten el robo de datos y la distribución de malware (Zhang et al., 2019). Se implementó también un algoritmo genético para generar muestras adversarias contra sistemas de detección de malware en IoT con Android, agregando características en el AndroidManifest.xml (Liu et al., 2019). Otros estudios utilizan CNN para detectar ataques de scanware en Android con buena eficiencia (Chen et al., 2018; Udayakumar et al., 2024; Vanjire y Lakshmi, 2024). Los modelos de Random Forest también se utilizan para la detección de aplicaciones, identificando patrones anómalos en transacciones (Ma et al., 2022).

2.2.4. Investigaciones relacionadas a los ataques de Sim Swapping

En el contexto del SIM Swapping, los ciberdelincuentes utilizan esta técnica para apoderarse de las líneas telefónicas de sus víctimas, con el objetivo de obtener la contraseña de un solo uso (OTP) generada por la institución financiera y, finalmente realizar operaciones electrónicas fraudulentas. Algunos estudios realizados, consideran fundamental un protocolo SMS seguro y la autenticación de dos factores, diseñado para ser accesible incluso para usuarios con baja alfabetización (Kisore y Sagi, 2015). Otro análisis destaca el aumento del SIM Swapping como un riesgo emergente, proponiendo medidas como una autenticación adicional del usuario además del autenticador de dos factores (2FA) (Kim et al., 2022). Por otro lado, se ha propuesto un diseño de billetera electrónica con un nivel de seguridad adicional basado en el IMEI del dispositivo, limitando su uso a un solo dispositivo para mitigar el riesgo de robo de la cuenta (Hassan y Shukur, 2021).

Finalmente, se ha desarrollado un sistema de prevención de fraude con SIM Box basado en el fingerprinting preciso de modelos de dispositivos, lo que permite la identificación confiable de dispositivos no autorizados (Oh et al., 2023). Se emplean también técnicas avanzadas de autenticación y mitigación de ciberataques en sistemas bancarios electrónicos, utilizando algoritmos basados en ML para detectar anomalías en transacciones, claves OTP, biometría y cifrado PKI, logrando una tasa de precisión del 95% mediante validación cruzada (Chaima et al., 2021). Otros trabajos también utilizan ML para la identificación del fraude de SIM Swapping, con procesos de mitigación inmediatos. Por ejemplo, un modelo basado en redes neuronales artificiales (ANN) logra una efectividad del 95.7% (Mathew, 2022), mientras que otro enfoque híbrido de ANN y RF alcanza una efectividad del 94% (Kala, 2021). Se han empleado técnicas avanzadas de análisis de datos basadas en el protocolo de capa de sockets seguros (SSL) y la autenticación de dos factores (2FA), logrando un 80% de efectividad (Monda, 2020). Finalmente, un modelo de Sistema de Autenticación Global Basado en Blockchain (BBGAS) propone el uso de biometría y tarjetas SIM para la identificación y mitigación de ciberataques (Khalili, 2022).

2.3. Bases teóricas

2.3.1. Fundamentos teóricos de la seguridad digital

2.3.1.1. Teoría de la seguridad en la información. La Teoría de la Seguridad de la Información, busca explicar cómo proteger la información de manera efectiva. Esta teoría se basa en los principios fundamentales como la confidencialidad, la integridad y la disponibilidad, y proporciona métodos y herramientas para evaluar y mitigar los riesgos de seguridad. (Whitman y Mattord, 2017)

2.3.1.2. Teoría de la gestión de riesgos en seguridad informática. La Teoría de la Gestión de Riesgos en Seguridad Informática es un enfoque sistemático para identificar, analizar, evaluar y tratar los riesgos de seguridad informática. Esta teoría proporciona un marco para tomar decisiones informadas sobre cómo proteger los activos de información de una organización (Hansford y Peltier, 2018)

2.3.1.3. Teoría de la ingeniería social. La Ingeniería Social es la manipulación psicológica de las personas para que revelen información confidencial o realicen acciones que de otra manera no realizarían. Los atacantes de ingeniería social aprovechan los sesgos cognitivos, las emociones y las debilidades humanas para lograr sus objetivos. (Mitnick y Vamosi, 2002)

2.3.1.4. Teoría de la innovación colectiva. Se basa en la idea de que el delito es un comportamiento aprendido. Los delincuentes aprenden sobre nuevas formas de delincuencia a través de su interacción con otros delincuentes y a través de los medios de comunicación. La teoría también sugiere que los delincuentes son más propensos a innovar si tienen acceso a oportunidades para hacerlo y si creen que sus innovaciones tendrán éxito. (Sutherland, 1958), teoría que también lo respaldan (Fernández y Rodríguez, 2017)

2.3.1.5. Teoría de la gestión de amenazas integradas. La Teoría de la Gestión de Amenazas Integradas (ITM, por sus siglas en inglés) propone la integración de varias funciones de seguridad informática, como firewalls, antivirus, antispyware, etc., en una única solución. Esta integración busca simplificar la gestión de la seguridad, reducir costos y mejorar la eficiencia en la detección y respuesta a amenazas (McBride, 2008).

2.3.2. Conceptos de la ciberseguridad y fraude digital

2.3.2.1. Delito. Se refiere a las actitudes humanas opuestas a la ley. Las leyes sólo establecen que hechos son delictivos e indica cuáles de estos hechos merecen ser denominados delitos. (Machicado, 2010)

2.3.2.2. Seguridad. Hace referencia al término seguro, que conceptualmente es estar en libertad y no estar sujeto a algún tipo de peligrosidad, daño o riesgo que pueda afectar alguna propiedad, interés o la misma existencia. (Saint-Pierre, 2008)

2.3.2.3. Ciberdelincuencia. La ciberdelincuencia se refiere a actividades delictivas que se llevan a cabo en el ciberespacio utilizando tecnologías de la información y comunicación. Estas actividades pueden incluir el robo de datos, el fraude en línea, el acceso no autorizado a sistemas informáticos, el malware, el phishing, entre otros. La ciberdelincuencia ha ido en aumento y representa una amenaza significativa para individuos, empresas y gobiernos en todo el mundo (Chang et ál., 2022).

2.3.2.4. Hacker. Se puede definir como un profesional de informática o experto que utiliza sus habilidades técnicas para llevar a cabo actividades en el ciberespacio, que pueden variar desde acciones maliciosas hasta acciones con motivaciones políticas o de aprendizaje, dependiendo del tipo de hacker en cuestión. (Chang et ál., 2022)

2.3.2.5. Hacking. El hacking se refiere al acto de buscar, identificar y explotar debilidades en sistemas informáticos o redes con el fin de obtener acceso no autorizado, manipular información o realizar acciones maliciosas. Los hackers pueden tener una variedad de motivaciones, que van desde la curiosidad y el aprendizaje hasta el robo de información, el sabotaje o la búsqueda de notoriedad. Es importante tener en cuenta que no todos los hackers tienen intenciones maliciosas, debido a que también existen hackers éticos que utilizan sus habilidades para mejorar la seguridad informática y proteger sistemas contra posibles ataques. (Chang et ál., 2022)

2.3.2.6. Aplicaciones móviles. Una aplicación móvil es un programa de software diseñado para ejecutarse en un dispositivo móvil, como un teléfono inteligente o una tableta. Las aplicaciones móviles suelen proporcionar funciones específicas y limitadas, como juegos, herramientas de productividad o acceso a redes sociales. (Dix et ál., 2004)

2.3.2.7. Transacción financiera. Una transacción financiera es una operación entre dos o más participantes en el que se intercambian bienes o servicios a cambio de un pago, es decir, una persona vende y la otra compra. (BBVA México, 2024)

2.3.2.8. Fraude cibernético. El fraude cibernético es el que se realiza mediante el uso de algún dispositivo conectado a internet. En la piratería informática, el ciberdelincuente utiliza diferentes herramientas para acceder a una computadora u otro dispositivo a distancia. (BBVA México, 2024)

2.3.2.9. Spoofing. Métodos que permiten imitar identidades a través de la falsificación de información en un proceso de comunicación (Nieto y Sánchez, 2023).

2.3.2.10. Phishing. La suplantación de identidad es un delito cibernético cada vez más sofisticado, involucra el envío de comunicaciones engañosas por parte de atacantes con el objetivo de obtener información confidencial de las víctimas. Este fenómeno se caracteriza por la utilización de sitios web y mensajes fraudulentos diseñados para adquirir datos personales con intenciones maliciosas. Ante la creciente complejidad y prevalencia de estos ataques, surge la necesidad de desarrollar sistemas de detección más avanzados, integrando tecnologías de inteligencia artificial y aprendizaje automático. (Seth y Madhavi, 2022)

2.3.2.11. Smishing. El concepto de smishing designa un tipo específico de fraude comunicacional donde los atacantes emplean mensajes SMS para inducir a los usuarios a revelar información sensible o ejecutar acciones malintencionadas. Esta técnica, una variante de la ingeniería social, busca principalmente adquirir credenciales de usuario, instalar software malicioso o preparar el terreno para ataques simulados más complejos. (Rahman et ál., 2023) Investigaciones recientes han abordado la dinámica y el impacto de estos ataques de suplantación de identidad, desarrollando simultáneamente métodos para contrarrestarlos (Timko y Rahman, 2023). Expertos han explotado diversos enfoques para mejorar la detección y prevención de ataques. Estos estudios indican que una proporción considerable de usuarios es susceptible a los ataques de smishing, lo que subraya la urgencia de fortalecer las estrategias de seguridad. Entre las propuestas más prometedoras se encuentran la implementación de clasificadores avanzados que analizan textos y URLs para identificar intentos de suplantación de identidad, y la aplicación de redes neuronales. Estas tecnologías, especialmente diseñadas para discernir patrones sutiles en el contenido

de los mensajes, prometen una alta precisión en la identificación y neutralización de intentos de smishing. El enfoque combinado de estas metodologías sugiere un avance significativo en la lucha contra la suplantación de identidad en entornos digitales.

2.3.2.12. *Vishing*. El vishing, término derivado de la fusión de voz y phishing, se refiere a una técnica de ingeniería social en la que el atacante, a través de llamadas telefónicas, busca persuadir a individuos específicos para que revelen información confidencial, como nombres de usuario y contraseñas, o datos sobre roles y responsabilidades de otros empleados. Durante estas interacciones, el visier emplea estrategias de manipulación y persuasión para obtener información que pueda ser utilizada para beneficio financiero inmediato o para facilitar la ejecución de ataques de vishing subsecuentes. Este método se caracteriza por su enfoque directo y personalizado, lo que potencialmente aumenta su efectividad en comparación con otras formas de ataques de phishing. La naturaleza de estas tácticas subraya la necesidad de una mayor conciencia y formación en seguridad informática para prevenir la divulgación no intencionada de información sensible (Armstrong et ál., 2023).

2.3.2.13. *Fuerza bruta*. La fuerza bruta es una metodología de hackeo que se utiliza para descifrar contraseñas, claves y credenciales de inicio de sesión (Giffary y Ramadhani, 2022). Es un método habitual utilizado por los ciberdelincuentes para obtener acceso no autorizado a las cuentas de usuario. Los ataques de fuerza bruta pretenden ser la forma más sencilla, barata y directa de acceder a un sitio web. Implica probar sistemáticamente todas las combinaciones posibles de contraseñas hasta encontrar la correcta. Los ataques de fuerza bruta se pueden utilizar para aprovechar las vulnerabilidades de los paquetes y recuperar datos importantes de los sistemas (Braslasu et al., 2023).

2.3.2.14. *Fake App*. Es una aplicación falsa que pretende ser legítima, pero que en realidad es maliciosa y tiene como objetivo engañar o dañar a los usuarios. Las aplicaciones falsas y las estafas en el sector bancario son dos áreas de preocupación distintas. Las aplicaciones falsas, que pertenecen a la industria móvil clandestina, han sido objeto de debates e

investigaciones limitados. (Tang et al., 2019). Es importante destacar que los cibercriminales desde líneas telefónicas que han sido activadas utilizando huellas de polímero o en establecimientos informales, envían el malware con ofertas engañosas de préstamos o promociones atractivas, persuadiendo a las víctimas para que descarguen e instalen una aplicación maliciosa. El propósito de esta acción es obtener el control total del dispositivo móvil, permitiendo la manipulación remota de las aplicaciones bancarias instaladas y facilitando la realización de operaciones fraudulentas a cuentas de terceros (cuentas mulas).

2.3.2.15. *Sim Swapping*. La técnica delictiva conocida como clonación de tarjetas SIM implica la reproducción no autorizada de tarjetas SIM para acceder ilegítimamente a servicios móviles y obtener datos personales y financieros confidenciales del titular de la línea. Esta práctica ha experimentado un notable incremento a nivel mundial, particularmente durante la pandemia de COVID-19, un periodo caracterizado por un aumento significativo de la dependencia en las comunicaciones y transacciones virtuales. Los criminales han explotado esta situación para intensificar sus actividades delictivas. (Park y Sangjin, 2023)

El proceso de clonación de tarjetas SIM se estructura generalmente en tres etapas clave: primero, la adquisición ilegítima de datos personales del usuario; segundo, la reproducción fraudulenta de la tarjeta SIM mediante técnicas sofisticadas; y tercero, la utilización de los servicios móviles usurpados para llevar a cabo actividades ilícitas. Este método representa un serio riesgo para la seguridad de la información y la privacidad de los usuarios, subrayando la necesidad de implementar medidas de seguridad más robustas tanto a nivel de operadores de servicios móviles como de los propios usuarios. (Park y Sangjin, 2023). Es crucial señalar que el cibercriminal tiene como objetivo apoderarse de la línea telefónica de su víctima para interceptar los códigos OTP enviados por las entidades financieras a través de mensajes de texto o recuperar las contraseñas bancarias. De esta manera, puede suplantar la identidad de la víctima y ejecutar operaciones fraudulentas a cuentas de terceros (cuentas mulas). Asimismo, algunos términos técnicos vinculados al cibercrimen se encuentran recopilados en el Anexo 1, titulado: *Glosario de Términos*, el

cual facilita la comprensión de los conceptos clave utilizados a lo largo de la presente investigación.

2.3.3. Contexto actual de la ciberseguridad y el comportamiento cibercriminal

En el contexto de la ciberseguridad y el comportamiento cibercriminal, el marco filosófico juega un papel crucial en la comprensión de los desafíos éticos y morales asociados con el uso de tecnologías avanzadas. En el caso de Hagendorff (2020) sostiene que las directrices éticas actuales en IA carecen de mecanismos efectivos para su implementación, lo que permite el abuso político y social de la tecnología. Propone que la ética debe ir más allá de los principios abstractos y enfocarse en la formación de caracteres y responsabilidades individuales en la creación y uso de tecnologías de IA. Este enfoque resuena con la filosofía de las virtudes, que enfatiza la importancia de cultivar virtudes tecno morales en los desarrolladores de IA para prevenir comportamientos cibercriminales y promover una conciencia ética (Hagendorff, 2020).

Robbins (2019), argumenta que la exigencia de explicabilidad para la IA puede ser errónea y debe aplicarse sólo a decisiones que tengan un impacto significativo. En el contexto del comportamiento cibercriminal, esto implica que las decisiones automatizadas deben ser explicables sólo si tienen un impacto significativo, además se sugiere una conciencia crítica sobre el uso de tecnologías avanzadas en la toma de decisiones, destacando la necesidad de transparencia y responsabilidad en los sistemas automatizados.

Danish y Herrera (2024), subrayan que la ciberseguridad en las prácticas de recursos humanos no solo es una cuestión técnica, sino también ética y filosófica. La proliferación de la tecnología digital y la dependencia de los sistemas informáticos en la gestión de datos sensibles exigen una conciencia ética y una responsabilidad colectiva. La capacidad de reconocer y mitigar amenazas cibernéticas refleja una comprensión profunda de la naturaleza del comportamiento cibercriminal y la necesidad de una cultura organizacional basada en la confianza, la transparencia y el respeto por la privacidad de los empleados.

Macnish y Van der Ham (2020) destacan las deficiencias en la gobernanza ética de la investigación en ciberseguridad, subrayando la falta de conciencia sobre los problemas éticos en la comunidad de la ciberseguridad. Abogan por una mayor educación ética en los cursos de ciencias de la computación y por el desarrollo de códigos de conducta efectivos. Además, enfatizan la necesidad de un diálogo activo sobre la ética en la ciberseguridad para mitigar el comportamiento cibercriminal y promover el uso consciente de la tecnología

Por otro lado, la corrupción, el fraude y el cibercrimen como fenómenos deshumanizantes. Dion (2011) argumenta que el cibercrimen implica una dualidad de intenciones y una mala fe, donde los criminales son conscientes de sus mentiras y manipulaciones. Esto no solo socava la confianza mutua en la sociedad, sino que también refleja un tipo de esclavitud moderna, donde los individuos se alienan de su propia humanidad y la de los demás a través del uso de la tecnología para explotar y dominar a otros. La discusión filosófica en torno a la ciberseguridad y el comportamiento cibercriminal resalta la necesidad de una ética robusta que guíe las acciones tecnológicas. Los principios filosóficos de las virtudes, la transparencia y la responsabilidad ética deben integrarse en el desarrollo y la implementación de tecnologías avanzadas para fomentar una cultura de responsabilidad y respeto por los derechos digitales. La educación ética y la promoción de virtudes tecno morales son esenciales para mitigar los riesgos asociados con el comportamiento cibercriminal y promover un uso más consciente y seguro de la tecnología. El modelo Sectrabank propuesto busca cumplir con la exigencia de la ética.

CAPÍTULO 3: ESTADO DEL ARTE

El fraude informático ha evolucionado significativamente en los últimos años debido al desarrollo de aplicaciones fraudulentas (Fake Apps) y ataques como el SIM Swapping. Estos métodos han sido analizados en diversas investigaciones que abordan técnicas de detección, mitigación y prevención. Estudios recientes han demostrado que técnicas de aprendizaje automático y profundo (ANN, CNN, RNN, etc.) han sido efectivas para detectar amenazas, aunque presentan desafíos como el alto poder computacional y la necesidad de grandes volúmenes de datos para su entrenamiento (Alshingiti et al., 2023; Ejaz et al., 2023). Por otro lado, técnicas híbridas que combinan métodos tradicionales con inteligencia artificial, como CNN-Transformer y Random Forest, han mostrado buenos resultados en la detección de phishing, smishing y otros fraudes electrónicos. Sin embargo, estos métodos aún enfrentan limitaciones en términos de adaptabilidad y costos computacionales. El presente estudio busca superar estas limitaciones mediante un modelo que no solo detecta sino también previene la materialización de los ataques, integrando múltiples capas de seguridad diseñadas específicamente para dispositivos Android.

3.1. Metodología para la revisión sistemática de la literatura

La revisión sistemática realizada en esta investigación se sustenta en el modelo metodológico propuesto por Kitchenham (2004), el cual se estructura en tres etapas claves. En la primera, correspondiente a la planificación, se formulan las preguntas centrales en torno a los objetivos del estudio y se define el enfoque de la revisión. La segunda fase, de ejecución, consiste en aplicar el plan establecido, seleccionando o descartando estudios de acuerdo con los criterios de inclusión y exclusión previamente definidos. Finalmente, en la etapa de reporte, se presentan los resultados obtenidos y la interpretación de los hallazgos. Para sistematizar la búsqueda de información se ha utilizado la herramienta informática Parsifal que es una herramienta web gratuita y colaborativa diseñada para apoyar la planificación y ejecución de revisiones sistemáticas de la literatura (RSL).

3.1.1. Planificación de la revisión sistemática de la literatura

Para la revisión sistemática de la literatura, vinculada al presente estudio de investigación, el análisis se ha estructurado en dos partes. La primera aborda las técnicas

de ataque como el phishing y el smishing, empleadas por los ciberdelincuentes para obtener información confidencial de las cuentas bancarias de sus víctimas. La segunda parte comprende los estudios relacionados con las modalidades de ataque SIM Swapping y Fake App, utilizadas para interceptar o secuestrar claves OTP y así ejecutar operaciones electrónicas fraudulentas, cuyas respuestas a las preguntas de investigación fueron obtenidas mediante una búsqueda sistemática en bases de datos de acceso abierto, específicamente en IEEE Xplore, ScienceDirect, MDPI y SpringerLink, Elsilver, Springer, ACM Journal seleccionando principalmente artículos científicos publicados en revistas de alto impacto, tesis, libros y reportes relevantes para el análisis. El periodo de publicación considerado abarca desde 2019 hasta 2025. La cadena de búsqueda para cada pregunta se presenta en la Tabla 1 y Tabla 2, y los criterios de inclusión y exclusión aplicados se describen en la Tabla 3.

3.1.1.1. Estudios relacionados con los ataques de phishing y smishing.

P1: ¿Qué técnicas se han implementado para identificar los ataques de Phishing en la banca móvil sobre dispositivos Android, y cuáles son la precisión, ventajas y limitaciones asociadas a dichas técnicas?

P2: ¿Qué técnicas se han implementado para identificar los ataques de Smishing en la banca móvil sobre dispositivos Android, y cuáles son la precisión, ventajas y limitaciones asociadas a dichas técnicas?

Tabla 1

Cadena de fuentes de búsqueda para phishing y smishing

Pregunta	Cadena
P1	("phishing" OR "spear-phishing" OR "email phishing" OR "phishing attacks" OR "phishing detection" OR "phishing mitigation") AND ("Model" OR "Modelo" OR Model*) AND ("Architecture" OR "Arquitectura" OR "system architecture" OR "arquitectura de sistema") AND ("Algorithm" OR "Algoritmo" OR Algorithm* OR "machine learning algorithm" OR "deep learning") AND ("Effectiveness" OR "Efectividad" OR "Evaluation" OR "Evaluación" OR "Performance") AND ("Implementation" OR "Implementación" OR "Deployment" OR "Despliegue") AND

	("Variables" OR "Features" OR "Indicadores" OR "Indicators" OR "Metrics" OR "Métricas")
P2	("smishing" OR "SMS phishing" OR "sms-phishing" OR "sms fraud" OR "sms scam" OR "text message phishing") AND ("Model" OR "Modelo" OR Model*) AND ("Architecture" OR "Arquitectura" OR "system architecture" OR "arquitectura de sistema") AND ("Algorithm" OR "Algoritmo" OR Algorithm* OR "machine learning" OR "deep learning") AND ("Effectiveness" OR "Efectividad" OR "Evaluation" OR "Evaluación" OR "Performance") AND ("Implementation" OR "Implementación" OR "Deployment" OR "Despliegue") AND ("Variables" OR "Features" OR "Indicadores" OR "Indicators" OR "Metrics" OR "Métricas")

3.1.1.2. Estudios relacionados con fraude informático en las modalidades de Fake Apps y SIM Swapping.

- P1:** ¿Qué técnicas se han implementado para mitigar el fraude informático en la modalidad de Fake App en la banca móvil sobre dispositivos Android, y cuáles son la precisión, ventajas y limitaciones asociadas a dichas técnicas?
- P2:** ¿Qué técnicas se han implementado para mitigar el fraude informático en la modalidad de SIM Swapping en la banca móvil sobre dispositivos Android, y cuáles son la precisión, ventajas y limitaciones asociadas a dichas técnicas?
- P3:** ¿Qué modelos, arquitecturas y algoritmos basados en técnicas de biometría han sido implementados para mitigar el fraude informático en aplicaciones bancarias Android, y cuáles son su efectividad, variables e indicadores de evaluación?
- P4:** ¿Qué modelos, arquitecturas y algoritmos basados en código IMEI han sido implementados para mitigar el fraude informático en aplicaciones bancarias Android, y cuáles son su efectividad, variables e indicadores de evaluación?
- P5:** ¿Qué modelos, arquitecturas y algoritmos basados en técnicas de geolocalización han sido implementados para mitigar el fraude informático en aplicaciones bancarias Android, y cuáles son su efectividad, variables e indicadores de evaluación?

P6: ¿Qué se ha reportado sobre la usabilidad y aceptación por parte de los usuarios al implementar medidas de seguridad multicapa?

Tabla 2

Cadena de fuentes de búsqueda para Fake App y SIM Swapping

Pregunta	Cadena
P1	("SIM swapping" OR "SIM swap" OR "SIM jacking" OR "SIM hijack" OR "port-out fraud" OR "port out attack" OR "suplantación de SIM") AND ("Technique Used" OR "Techniques Used" OR "Técnica utilizada")AND ("Accuracy" OR "Precisión") AND ("Advantages" OR "Benefits" OR "Ventajas") AND ("Limitations" OR "Constraints" OR "Limitaciones" OR "usability")AND ("Scam Bank" OR "computer fraud")
P2	("fake app" OR "fake application" OR "malicious app" OR "malicious application" OR "fake banking app" OR "trojanized app" OR "repackaged app" OR "APK repackaging" OR "fraudulent app" OR "cloned app") AND ("Technique Used" OR "Techniques Used" OR "Técnica utilizada" OR "Técnicas utilizadas") AND ("Accuracy" OR "Precisión" OR "Precision" OR "usability") AND ("Advantages" OR "Benefits" OR "Ventajas") AND ("Limitations" OR "Constraints" OR "Limitaciones")AND ("Scam Bank" OR "computer fraud")
P3	("biometric security" OR "biometric authentication" OR "biometrics" OR "biometric system" OR "biometric protection" OR "seguridad biométrica" OR "autenticación biométrica")AND ("Model" OR "Modelo")AND ("Architecture" OR "Arquitectura")AND ("Algorithm" OR "Algoritmo" OR "Algorithms" OR "Algoritmos")AND ("Effectiveness" OR "Eficacia" OR "Effectiveness" OR "Evaluation" OR "Evaluación" OR "Performance" OR "usability") AND ("Implementation" OR "Implementación" OR "Deployment" OR "Despliegue")AND ("Variables" OR "Indicadores" OR "Indicators")
P4	("IMEI" OR "IMEI code" OR "IMEI number" OR "International Mobile Equipment Identity" OR "número IMEI" OR "código IMEI" OR "identificador del equipo móvil")AND ("Model" OR "Modelo" OR "Model*")AND ("Architecture" OR "Arquitectura" OR "System architecture" OR "Arquitectura de sistema")AND ("Algorithm" OR "Algoritmo" OR "Algorithms" OR "Algoritmos" OR "Método") AND ("Effectiveness" OR "Efectividad" OR "Evaluation" OR "Evaluación" OR "Performance" OR "usability") AND ("Implementation" OR "Implementación" OR "Deployment" OR "Despliegue") AND ("Variables" OR "Indicadores" OR "Indicators" OR "Metrics" OR "Métricas")
P5	("geolocation security" OR "location security" OR "seguridad de geolocalización" OR "seguridad de ubicación" OR "location-based security" OR geofencing OR geofence) AND ("Model" OR "Modelo" OR Model* OR "Modeling")AND ("Architecture" OR "Arquitectura" OR "system architecture" OR "arquitectura de sistema")AND ("Algorithm" OR "Algoritmo" OR Algorithms OR Algoritmos)AND ("Effectiveness" OR "Efectividad" OR "Evaluation" OR "Evaluación" OR Performance OR Rendimiento OR "usability")AND ("Implementation" OR "Implementación" OR Deployment OR Despliegue) AND ("Variables" OR "Indicadores" OR "Indicators" OR "Metrics" OR "Métricas")

P6	("biometric security" OR "biometric authentication" OR biometrics OR "seguridad biométrica" OR "autenticación biométrica")
	AND ("IMEI" OR "IMEI code" OR "IMEI number" OR "International Mobile Equipment Identity" OR "número IMEI" OR "código IMEI")
	AND ("geolocation security" OR "location security" OR geofencing OR "seguridad de geolocalización" OR "seguridad de ubicación")
	AND ("usability" OR "usability testing" OR "usability evaluation" OR "usabilidad" OR "experiencia de usuario" OR "UX")
	AND ("banking application" OR "banking applications" OR "mobile banking" OR "bank app" OR "aplicaciones bancarias" OR "banca móvil")

Tabla 3
Criterios de inclusión y exclusión

Criterio de Inclusión	Criterio de Exclusión
Publicaciones entre 2019 y 2025	Publicaciones de artículos de contribución mayor a 5 años
Artículos científicos revisados por pares, journals , congresos, libros y tesis.	Revisiones de literatura no sistemáticas
Estudios que describen técnicas, métodos y modelos para mitigar fraude en banca móvil específicamente de Fake App y SIM Swapping	Estudios de informática distinto al campo de ciberseguridad
Estudios que estén relacionados con las preguntas de investigación.	Revisión sistemática de la Literatura

3.1.2. Ejecución de la revisión sistemática de la literatura

Para la fase de ejecución, se llevó a cabo un riguroso proceso de selección basado en los criterios de inclusión y exclusión previamente establecidos, con el propósito de identificar los estudios relacionados con la presente investigación, centrada en el fraude informático mediante las modalidades de Fake App y SIM Swapping.

Asimismo, se buscó incluir aquellos trabajos que aportaran información clave como la técnica utilizada, precisión, ventajas, limitaciones, referencia, descripción del modelo, arquitectura, algoritmo, efectividad, implementación y variables o indicadores.

El procedimiento aplicado y los resultados obtenidos en cada etapa se muestran en la Figura 5. Posteriormente, se realizó un análisis exhaustivo de los artículos que respondían a las preguntas de investigación, partiendo de un total inicial de 1,483 artículos. De estos, se

seleccionaron 105 artículos, 15 libros y 7 tesis, conformando un total de 127 referencias que cumplieron con los criterios de inclusión y exclusión definidos, tal como se detalla en la Tabla 4.

Figura 5
Proceso de revisión de la literatura

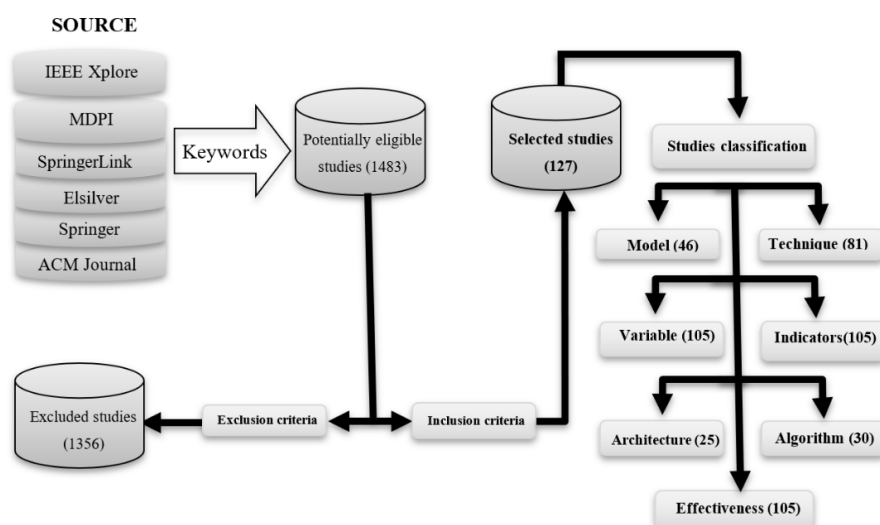


Tabla 4
Fuente de artículos seleccionados

Fuente	Estudios potencialmente elegibles	Estudios seleccionados (Journal article)
MDPI	298	27
Elsilver	208	17
IEEE Xplore	180	15
SpringerLink	146	6
ACM Journal	164	6
Otros	487	34
Total	1483	127

3.1.3. Resultados de la búsqueda de la revisión sistemática de la literatura

Durante el proceso de revisión sistemática de la literatura orientado al desarrollo del modelo Sectrabank, se seleccionaron y analizaron un total de 127 referencias bibliográficas. De este conjunto, 105 corresponden a artículos científicos publicados en revistas indexadas, complementados por 15 libros especializados, 7 tesis académicas y una

serie de reportes técnicos de alto rigor metodológico. La distribución de estas fuentes, representada en los gráficos correspondientes, evidencia el sólido sustento académico y técnico que respalda la presente investigación, garantizando un enfoque integral, actualizado y riguroso para abordar el problema del fraude informático en aplicaciones de banca móvil, cuyos reportes se muestran en las figuras 6, 7 y 8.

Figura 6
Cantidad de artículos por base de datos

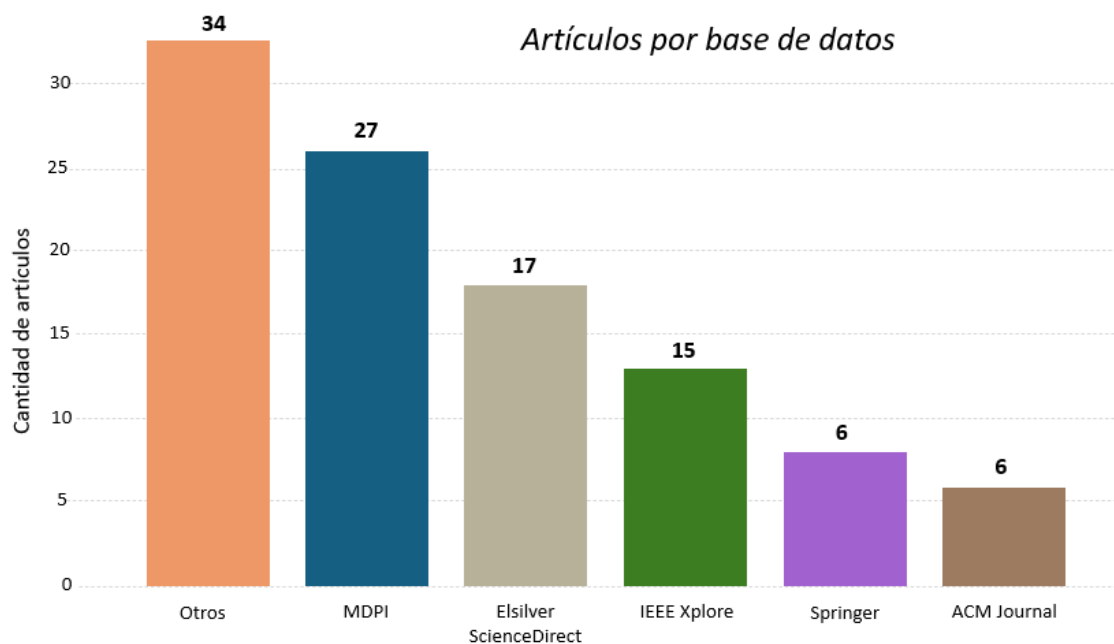


Figura 7
Cantidad de artículos por revista

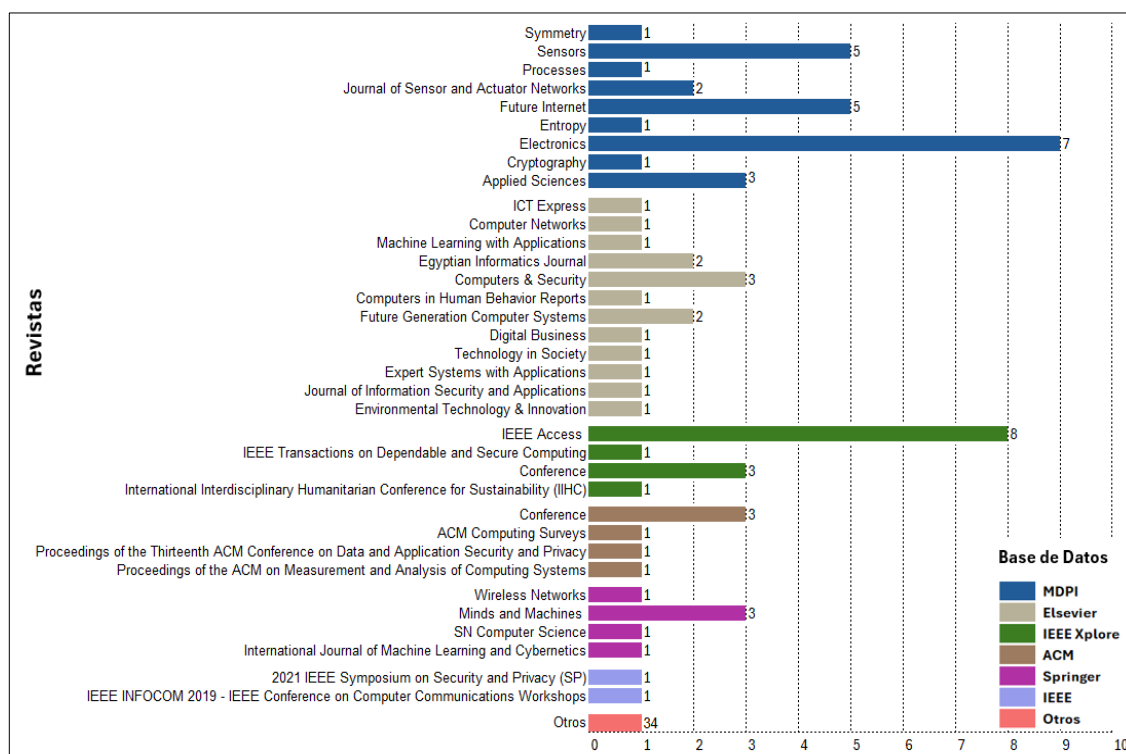
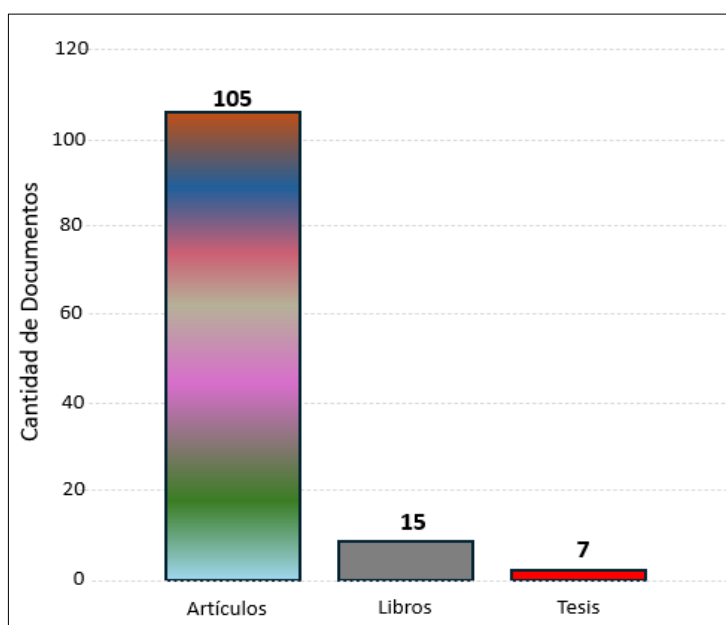


Figura 8
Cantidad de artículos, libros y tesis



3.1.3.1. Reporte de los estudios relacionados a los ataques de phishing

Los estudios analizados destacan el uso de modelos como CNN, LSTM, Transformers, Random Forest y BERT, que han logrado precisiones superiores al 95%, demostrando una alta capacidad para identificar patrones maliciosos en URLs, correos o aplicaciones falsas. Modelos híbridos como los propuestos por Alshingiti et al. (2023) y Asiri et al. (2023), que combinan CNN, LSTM y Transformers, alcanzaron niveles de precisión cercanos al 99%, mostrando gran efectividad en la detección automatizada de amenazas sin necesidad de ingeniería manual. Asimismo, Elsadig et al. (2022) y Alqahtani et al. (2022) demostraron que la integración de modelos como BERT + CNN o DAE + AAA + IWO mejora la precisión y optimiza la selección de características, aunque siguen dependiendo de la calidad del dataset y presentan un consumo computacional elevado. Por otro lado, métodos más tradicionales como Random Forest, RFE o Ensemble Learning, empleados por autores como Alani y Tawfik (2022) y Kalabarige et al. (2022), ofrecen un equilibrio entre precisión y eficiencia, con resultados entre 97% y 99%. En general, los hallazgos muestran que, si bien las técnicas actuales son altamente efectivas en la detección del phishing, enfrentan limitaciones vinculadas a la complejidad de implementación, la dependencia de grandes datasets y la capacidad de adaptación frente a amenazas emergentes, cuyo reporte se aprecia en la tabla 5.

Tabla 5
Ataques de Phishing con sus ventajas y limitaciones

Referencia	Técnica Utilizada	Precisión	Ventajas	Limitaciones
(Alshingiti et al., 2023)	CNN, LSTM y LSTM–CNN	CNN: 99.2% LSTM–CNN: 97.6% LSTM: 96.8%	Detecta patrones sin ingeniería manual CNN eficiente en phishing LSTM útil para URLs	Requiere grandes datasets Alto consumo computacional Vulnerable a cambios en phishing

(Ejaz et al.,2023)	Learning without Forgetting (LWF) y Elastic Weight Consolidation (EWC)	LWF 94%, EWC 93%	Permite adaptación a nuevas tareas sin olvidar completamente las anteriores	Aumento de parámetros, Olvido de datos
(Asiri et al.,2023)	CNN-Transformer	99%	Combinación de CNN y Transformer mejora la precisión	Tamaño del pipeline de entrada, Costo computacional elevado, Necesidad de optimización del tamaño de entrada
(Roy et al, 2022)	LSTM	99%	Buen rendimiento en secuencias Funciona con datasets pequeños	Costoso en predicción Sensible al ruido
(Elsadig et al.,2022)	BERT + CNN	96.66%	Alta precisión en URLs de phishing	Requiere hardware especializado Depende de la calidad del dataset
(Alqahtani et al.,2022)	DAE + AAA + IWO	99.28%	Aprendizaje profundo Selección óptima de características	Alto consumo computacional
(Almseidin et al,2022)	Fuzzy Rule Interpolation (FRI)	97.58%	Reducción de falsos positivos Manejo efectivo de incertidumbre Mejora la detección en escenarios de información incompleta	Parámetros fuzzy requieren ajuste Ineficiente con grandes volúmenes
(Alani y Tawfik,2022)	Random Forest + RFE	97.50%	Menos características mejoran eficiencia Desplegable en la nube	Requiere actualización constante
(Kalabarige et al.,2022)	MLSELM (Ensemble Learning)	D1: 97.76% D2: 98.90% D3: 96.79% D4: 98.43%	Usa múltiples clasificadores Técnicas de balanceo de datos.	Alto costo computacional Menos eficiente en tiempo real
Almuhaideb et al.,2022)	Random Forest + Hashing	99.80%	Alta precisión en ataques homogélicos Aprendizaje continuo	Difícil de interpretar Vulnerable a envenenamiento de datos
(Mohamed et al.,2022)	NN, SVM, RF + heurística y listas negras	NN: 95.18% SVM: 85.45% RF: 78.89%	Detecta phishing de día cero Usa múltiples clasificadores	Depende de listas negras Falsos positivos en heurística

(Aljofey et al, 2020)	CNN	95.02% (propio) 98.58% (D2) 95.46% (D3) 95.22% (D4)	No requiere acceso al contenido web Detecta patrones sin conocimiento previo Respuesta rápida en cliente	Tiempo de entrenamiento largo No verifica si la URL está activa Dificultad con URLs cortas
(Panda et al.,2022)	Procesamiento de imágenes y RF	87%	Usa reconocimiento visual para detectar phishing	Precisión limitada, Datos de entrenamiento limitados, Pocos modelos ML usados
(Moedjahedy et al.,2022)	Machine Learning	97.07%	Alta precisión en clasificación de sitios	No hay método único, Alta dimensionalidad de datos, Evolución del phishing
(Liu y Fu,2020)	SPWalk (graph-based)	>95% precisión, ~84% recall, F1-score alto	Reduce efecto de camuflaje Escalable a redes grandes	Afectado por puntuaciones inexactas
(Sathya et al,2020)	Random Forest + NLP	98.38%	No accede al contenido web Clasifica en benigno, spam y malicioso	Sensible a ofuscación de URLs No detecta malware
(Sahingoz et al, 2019)	Random Forest + NLP	97.98%	Independencia del idioma Detección en tiempo real Eficaz contra-ataques zero-day	No detecta URLs simples Requiere dataset amplio

3.1.3.2. Reporte de estudios relacionados a los ataques de Smishing

Entre las técnicas más efectivas destacan las combinaciones de CNN y LSTM, que, según Ghourabi et al. (2023) y Stevanović (2022), alcanzan precisiones superiores al 98%, demostrando una notable capacidad para reconocer patrones ocultos en mensajes de texto. Otros enfoques, como los de Akande et al. (2023) y Qi et al. (2023), utilizaron algoritmos basados en reglas y muestreo estocástico (RIPPER, FMMPED), logrando precisiones cercanas al 98%, aunque enfrentan falsos positivos y dependencia del conjunto de datos. De manera similar, Shaukat et al. (2023) y Gualberto et al. (2020) aplicaron XGBoost, destacando su eficiencia para manejar datos desbalanceados, aunque con riesgo de sobreajuste y alto costo computacional. Asimismo, propuestas como las de Althobaiti et al. (2023) introdujeron técnicas de clustering sin etiquetas previas, que ofrecen una alternativa prometedora ante la falta de datos etiquetados, aunque con un rendimiento inferior (82%) debido a su alto costo de procesamiento y necesidad de etiquetado manual parcial, cuyos resultados en forma detallada se muestra en la tabla 6

Tabla 6
Ataques de Smishing con sus ventajas y limitaciones

Referencia	Técnica Utilizada	Precisión	Ventajas	Limitaciones
(Akande et al.,2023)	Algoritmo RIPPER y C4.5	98.08%	Generación de reglas basadas en patrones.	Falsos positivos y negativos. - Dependencia del conjunto de datos UCL SMS spam. - Requiere mantenimiento constante de reglas.
(Shaukat et al.,2023)	XGBoost	94%	Modelo altamente optimizado.	Alto consumo computacional. - Sensibilidad al ajuste de hiperparámetros. - Riesgo de sobreajuste.
(Althobaiti et al.,2023)	Mean Shift y DBSCAN	82%	Clustering para detección sin etiquetas previas.	Alto costo computacional. - Datos limitados. - Etiquetado manual parcial.
(Qi et al.,2023)	Algoritmo FMMPED	97.97%	Estrategia de muestreo de Markov para optimización.	Dependencia de la calidad del submuestreo. - Ajuste fino de parámetros. - Costo computacional elevado.
(Ghourabi et al.,2023)	CNN y LSTM	98.38%	Deep learning mejora la detección.	Alto consumo de recursos. - Dependencia del conjunto de datos. - Vulnerabilidad a ataques adversariales.
(Stevanović,2022)	LSTM y CNN	99.81%	Combinación de deep learning para mejorar detección.	Alto costo computacional. - Dificultad de interpretación. - Dependencia de grandes volúmenes de datos.
(Mambina et al.,2022)	Extra Trees	99.80%	Uso de Random Forest para mejorar la precisión.	Enfoque limitado a suajili. - Sesgo en la recolección de datos.
(Sonowal,2020)	BSFS	97.41%	Optimización en la selección de características.	Dependencia de la selección de características. Riesgo de eliminar características útiles.
(Gualberto et al.,2020)	XGBoost y LNP	99.95%	Excelente manejo de datos desbalanceados.	Riesgo de sobreajuste. - Alto consumo computacional. - Sensibilidad a datos

desequilibrados.				
(Mishra y Soni,2020)	Análisis de código fuente, URLs y análisis de APK maliciosos	96.29%	Enfoque basado en múltiples fuentes de datos.	Alto consumo de recursos. - Dependencia del conjunto de datos
(Sonowal,2020)	Algoritmos de correlación y ML	98.40%	Reducción del número de características en 61.53%.	Dimensión de características sigue siendo alta. - Dependencia del clasificador AdaBoost. - Limitaciones en la selección de características.

3.1.3.3. Reporte de estudios relacionados a los ataques de Fake App

Los estudios más recientes demuestran que las técnicas de inteligencia artificial superan ampliamente el 95 % de precisión en la detección de fraudes mediante Fake Apps, consolidándose como herramientas clave en la seguridad bancaria móvil. Vanjire y Lakshmi (2024) alcanzaron más del 99 % al combinar CNN con sistemas explicables de IA (XAI), aunque su ejecución requiere alta capacidad de GPU. De forma similar, Udayakumar et al. (2024) integraron GIST, FFNN y Random Forest, logrando 98 % de efectividad, pero con la limitación de necesitar acceso total a los archivos APK o DEX. Por otro lado, Prayogi y Aji (2023) propusieron el método Mobile Network Verification (MNV), con un 100 % de detección, aunque su aplicación depende de políticas y redes móviles activas. En la misma línea, Anjum et al. (2022), con Bayesian Neural Networks (BNN), superaron el 99 %, a costa de un alto consumo de recursos. Modelos como el Árbol de Diseño Fusiónado (MLT) de Xie et al. (2021) o el uso de RNN y CFG de Ullah et al. (2021) ofrecieron buen desempeño, aunque con riesgo de falsos positivos y alto costo computacional. Finalmente, enfoques tradicionales como los de Gezer et al. (2019) y Zhang et al. (2019), basados en Random Tree, Naive Bayes y firmas digitales, lograron resultados entre 83 % y 91 %, pero se muestran insuficientes ante las sofisticadas técnicas de ofuscación actuales, cuyos resultados en forma detallada se muestra en la tabla 7

Tabla 7
Ataques de Fake App con sus ventajas y limitaciones

Referencia	Técnica Utilizada	Precisión	Ventajas	Limitaciones
(Udayakumar et al.,2024)	GIST (Global Image Shape Transform), FFNN y Random Forest	98%	Buen desempeño en detección	Requiere acceso al archivo APK/DEX completo
(Vanjire y Lakshmi,2024)	CNN combinado con XAI	>99%	Alta precisión en detección y clasificación	Requiere recursos significativos de GPU para el entrenamiento
(Prayogi y Aji,2023)	Mobile Network Verification (MNV)	100%	Alta efectividad	Requiere políticas gubernamentales y solo funciona con datos móviles
(Anjum et al.,2022)	BNN	>99%	Buen rendimiento en detección	Requiere grandes volúmenes de datos y potencia computacional
(Xie et al.,2021)	Árbol de diseño fusionado (MLT)	99%	Fusión dinámica de información UI	Puede generar falsos positivos en apps con interfaces limitadas
(Ullah et al.,2021)	Control Flow Graph (CFG) y RNN	96.24%	Buen desempeño en detección	El análisis CFG es costoso en términos computacionales para aplicaciones grandes
(Arslan,2021)	Deep Learning (DNN - Deep Neural Network)	99.24%	Alto desempeño en detección	Se basa solo en análisis estático, sin incorporar análisis dinámico
(Wu et al.,2020)	TLSH y MinHash	>99%	Alta precisión en detección	No se especifica la cantidad de ruido o falsos positivos en un entorno en vivo
(Liu et al.,2020)	Network Embedding	>95%	Uso de técnicas avanzadas de embedding	Alto costo computacional por el cálculo de probabilidades de transición
(Gezer et al.,2019)	Random Tree (RT), J48, Naive Bayes (NB), SMO	RT: 83%, J48: 77%, NB: 64%, SMO: 60%	Se analizaron 41,437 muestras, de las cuales 13,077 fueron funcionales	La mejor precisión alcanzada fue del 83%, dejando un 17% de margen de error
(Zhang et al.,2019)	Análisis de virtualización y firma digital	91.11%	Identificación basada en firmas digitales	Algunos malwares siguen evadiendo la detección

3.1.3.4. Reporte de estudios relacionados a los ataques de SIM Swapping

Los estudios más recientes, como el de Oh et al. (2023), aplicaron técnicas de model checking con UPPAAL y device fingerprinting, alcanzando una precisión del 100% en la identificación de cambios sospechosos de dispositivos, aunque su efectividad depende del tamaño y diversidad del conjunto de huellas digitales recopiladas. De forma complementaria, Kim et al. (2022) propusieron un esquema de autenticación multifactor (MFA) basado en biometría, tokens físicos y blockchain, que incrementa la seguridad, pero presenta altos costos de implementación e infraestructura compleja para un despliegue masivo. Asimismo, Hassan y Shukur (2021) lograron también un 100% de efectividad al combinar MFA con cifrado RSA y Firebase, ofreciendo una protección robusta en entornos de transacción digital, aunque su funcionamiento depende de plataformas externas como Firebase y PayPal. Por su parte, Kala (2021) introdujo el uso de redes neuronales artificiales (ANN) y Random Forest, con una precisión del 94%, demostrando la utilidad de la inteligencia artificial para detectar patrones de fraude, aunque su eficacia requiere la cooperación de los operadores de red. En los trabajos pioneros, Kisore y Sagi (2015) propusieron un protocolo de acuerdo de claves EC-MQV y cifrado AES de 256 bits, alcanzando una seguridad reforzada en autenticaciones de bajo valor, aunque con vulnerabilidades frente a malware y estaciones base falsas, cuyos resultados en forma detallada se muestra en la tabla 8

Tabla 8
Ataques de SIM Swapping con sus ventajas y limitaciones

Referencia	Técnica Utilizada	Precisión	Ventajas	Limitaciones
(Oh et al.,2023)	Model checking con UPPAAL, Device fingerprinting	100%	Alta efectividad en la detección de cambios sospechosos en dispositivos	La efectividad depende del tamaño del dataset de fingerprints, que puede no cubrir todos los dispositivos del mercado.

(Kim et al.,2022)	Autenticación multifactor (MFA), implementación de biometría y tokens físicos, uso de blockchain para la verificación de identidad	85%	Aumenta la seguridad con múltiples factores de autenticación y tecnología blockchain	La biometría y los tokens físicos pueden ser costosos y difíciles de implementar a gran escala. El monitoreo en tiempo real requiere infraestructura avanzada y puede generar falsos positivos.
(Hassan y Shukur.,2021)	Autenticación multifactor (MFA), Cifrado RSA y Firebase	100%	Seguridad robusta mediante MFA y cifrado fuerte	Dependencia de la infraestructura de Firebase y PayPal para la seguridad y las transacciones.
(Kala,2021)	Redes neuronales artificiales (ANN) y RF	94%	Aplicación de técnicas de inteligencia artificial para la detección de fraudes	Dependencia de la cooperación de los operadores de red para compartir datos.
(Kisore y Sagi,2015)	Protocolo de acuerdo de claves EC-MQV, cifrado AES de 256 bits, autenticación de dos factores (IMSI + contraseña)	90%	Mayor seguridad en autenticación mediante cifrado avanzado	Limitado a transacciones de bajo valor (máximo \$200 por transacción), vulnerable a malware y ataques de estaciones base fantasmas

3.1.3.5. Reporte de estudios relacionados con modelos de seguridad biométrica

Entre los avances más destacados, Awad et al. (2024) desarrollaron un sistema multimodal que combina reconocimiento facial y de huellas dactilares, alcanzando precisiones del 93 % al 97 % mediante arquitecturas IoT y CNN, aunque exige un control riguroso de errores (FAR, FRR, EER). Khan et al. (2023) resaltaron la eficacia de la autenticación multifactor (MFA), que incrementó la seguridad en 46 %, mientras que Ali et al. (2021) integraron PIN, OTP y biometría bajo un esquema criptográfico robusto (SHA-256, RSA, FIDO) para reforzar la protección móvil. De forma complementaria, Lien y Vhaduri (2023) y Bedari et al. (2022) lograron altas precisiones en autenticación por huella, destacando este último con EER inferiores al 1 % mediante plantillas cancelables en redes 5G. Finalmente, Bairwa y Joshi (2021) propusieron un protocolo de autenticación mutua con huellas, dirección MAC y tokens, mejorando la integridad de los nodos distribuidos., cuyos resultados en forma detallada se muestra en la tabla 9

Tabla 9
Análisis comparativo de modelos biométricos

Referencia	Descripción del modelo	Arquitectura	Algoritmo	Efectividad	Implementación	Variables/Indicadores
Awad et al. (2024)	Desarrollan un sistema de autenticación biométrica multimodal en IoT que combina reconocimiento de huellas dactilares y facial	Se adopta una arquitectura distribuida donde la extracción de características ocurre en dispositivos IoT locales y la comparación se realiza en un servidor en la nube	Se utilizan algoritmos de aprendizaje profundo CNN para extraer rasgos faciales y métodos clásicos de visión (clasificador en cascada de Haar y LBPH para reconocimiento facial)	Los sistemas reportan alta precisión: por ejemplo, un sistema multimodal alcanzó un 93–97 % de exactitud y otro logró 96 % de precisión en un entorno de salud personalizado	Se implementó un robot equipado con sensor infrarrojo pasivo y cámara que transmite video en tiempo real vía IoT, con interfaz web de control remoto por Wi-Fi	Entre los indicadores analizados se incluyen la precisión (accuracy) del reconocimiento y las tasas de aceptación/rechazo falso (FAR/FRR), además de la tasa de error igualado (EER) para balance de desempeño
Khan et al. (2023)	El modelo propuesto integra autenticación multifactor (MFA) para fortalecer la seguridad de transacciones móviles, en Fin-Tech.	Se basa en una revisión sistemática de literatura (SLR) de 92 estudios sobre autenticación en transacciones móviles.	No desarrolla un algoritmo propio; analiza mecanismos existentes como OTP, biometría, blockchain y quantum OTP.	Se menciona que el uso de QR y MFA incrementó la seguridad de las transacciones en un 46%	La implementación es conceptual, enfocada en la síntesis crítica de técnicas y enfoques actuales	Tipo de autenticación, nivel de efectividad y mitigación de riesgos fueron los principales indicadores analizados.

Lien y Vhaduri (2023)	Se basa en el análisis de patrones de huella, con características globales (patrones de crestas) y locales (minutiae únicas).	Implementaron un sistema que realiza 125,000 comparaciones/seg en un PC Pentium D a 2.80 GHz (1 GB RAM), ilustrando la capacidad del hardware utilizado	Emplea emparejamiento de minutiae (cálculo de distancia euclidiana y diferencia angular de minutiae), correlación cruzada de las imágenes de huella, y redes neuronales entrenadas para calcular un score de similitud	El artículo sólo indica un “alto nivel de precisión” sin reportar un porcentaje numérico de eficacia	Se implementa con pequeños escáneres de huella integrados en dispositivos IoT que capturan las huellas con alta precisión	Cada minutia se representa con coordenadas (x_i , y_i) y orientación (θ_i), y la similitud global $S(T,I)$ entre huellas sirve como indicador de correspondencia
Bedari et al. (2022)	Sistema de autenticación de huellas para IIoT en 5G, usando plantillas cancelables que protegen las características biométricas.	Dispositivos IIoT extraen huellas y envían plantillas cifradas por 5G a la nube, donde se realiza la comparación y verificación	Utiliza un algoritmo de reordenamiento y promediado de vectores de características de huellas basado en MCC para proteger datos	El sistema logró EER entre 0.04 % y 0.99 %, manteniendo alta precisión de autenticación aún usando plantillas	Integra extracción de minucias con SDK VeriFinger, generación de plantilla en el borde y comparación segura en la nube 5G.	Evaluaron FAR (Tasa de Falsa Aceptación), FRR (Tasa de Falso Rechazo), EER (Tasa de Error Igual), tiempos de procesamiento y tamaño de plantilla, demostrando eficiencia en precisión y velocidad.
Ali et al. (2021)	Desarrollan un algoritmo de autenticación	Incluye aplicaciones móviles (G-	Opera en tres fases (registro, autenticación y	No reporta un porcentaje exacto, pero	Se desarrollaron prototipos móviles G-MoMo usando	Utiliza PIN, OTP, huella biométrica, número de serie SIM, ID de usuario y

	multifactor que integra PIN, OTP y biometría para asegurar aplicaciones de dinero móvil.	MoMo), servidores, bases de datos principales y sistemas FIDO para reforzar la autenticación.	transacción) usando SHA-256, RSA, FIDO y Fernet para cifrado de datos.	afirma alta eficiencia y seguridad contra ataques comunes	Twilio para OTPs, códigos QR como bases de datos cifradas y biometría de smartphones.
Bairwa y Joshi (2021)	Proponen un protocolo de autenticación mutua de nodos utilizando dirección MAC, huella dactilar y token de sesión.	Incluye un nodo que monitoriza MACs y firmas digitales basadas en la combinación de MAC y huella dactilar.	Conjunto de subalgoritmos para registro, validación de MAC, generación de tokens, cifrado de mensajes y verificación de integridad.	Se mejoró la entropía de claves hasta 209 bits, aunque no se reporta un porcentaje de efectividad global.	Simulado en MATLAB con interfaces gráficas para registro, validación de nodos y pruebas de seguridad de contraseñas.

3.1.3.6. Reporte de estudios relacionados con modelos de seguridad por código IMEI

Los estudios revisados evidencian que el código IMEI se ha convertido en un elemento esencial para fortalecer la autenticación multifactor en dispositivos móviles. Modelos como SAM-PAY (Berbecaru, 2025) y Zamwallet (Hassan y Shukur, 2022) demostraron su eficacia al integrar IMEI, OTP, huella y localización certificada, garantizando autenticaciones seguras y personalizadas. Propuestas como la de Zukarnain et al. (2022), que incorporan mobile identity con IMEI, SIM y GPS, amplían su aplicabilidad en entornos reales. Finalmente, Alsunaidi y Almuhaideb (2021) introdujeron el uso de blockchain permitida para registrar y validar la identidad de los dispositivos. En conjunto, los modelos basados en IMEI mejoran la confianza y trazabilidad, aunque enfrentan desafíos de privacidad, interoperabilidad y dependencia tecnológica, cuyos resultados en forma detallada se muestra en la tabla 10

Tabla 10
Análisis comparativo de modelos por código IMEI

Referencia	Descripción del modelo	Arquitectura	Algoritmo	Efectividad	Implementación	Variables/Indicadores
Berbecaru (2025)	Desarrollan SAM-PAY que es un método de autenticación multifactor que combina localización certificada, PIN, OTP y el dispositivo móvil	Integra terminales GNSS, un Elemento Local para certificar ubicación, middleware distribuido y un Proveedor de Servicios.	Modifica el algoritmo LDEA aplicando operaciones XOR y SHA-256 sobre coordenadas para cifrar dinámicamente la OTP.	No se reporta porcentaje explícito; se menciona solo la factibilidad y efectividad demostrada en pruebas reales.	Se desarrolló un prototipo completo combinando dispositivos A-GPS, comunicaciones móviles y servidores SP y LE.	Credenciales, IMEI, datos bancarios, claves compartidas, coordenadas certificadas y la OTC son variables clave.
Hassan y Shukur (2022)	Desarrollan un esquema de autenticación multifactor para e-wallets basado en IMEI, contraseña, huella digital y OTP	La app Android se conecta a Firebase en la nube y usa PayPal como pasarela de pagos	Se emplea cifrado RSA de clave pública (ej. 2048 bits) para proteger contraseñas y comunicaciones	No se reporta porcentaje; solo se menciona que todas las pruebas funcionales fueron exitosas	Se creó la app “Zamwallet” en Android Studio con módulos de registro, login, perfil, recarga y transferencia	Contraseña, OTP, huella dactilar del usuario y el IMEI como identidad única del dispositivo

Zukarnain et al. (2022)	Proponen “mobile identity” como entidad de autenticación adicional para equilibrar seguridad y conveniencia	Sistema cliente-servidor donde un servidor de autenticación (AS) verifica credenciales y emite un token cifrado.	Usa la huella para cifrar datos mediante cifrado asimétrico y generar un token validado por el servidor de aplicaciones.	No se reportan porcentajes de efectividad; el artículo se centra en el diseño conceptual	Se presentan ejemplos de código de Android/iOS que acceden a SIM, IMEI, huellas y GPS, generando tokens cifrados.	SIM, IMEI, huellas dactilares, ubicación y la generación de un token cifrado como indicador de autenticación exitosa.
Alsunaidi y Almuhaideb (2021)	Desarrollan un esquema de autenticación de smartphones usando blockchain permissionada con protocolos de registro, transferencia de propiedad y acceso a red celular.	Utiliza una blockchain de consorcio administrada por agencias gubernamentales, con registros de dispositivos y gestión de propiedad mediante smart contracts.	Emplea una criptografía de clave pública y funciones hash para firmar y verificar la identidad de cada smartphone en la red blockchain	No se reportan métricas cuantitativas; solo se mencionan descripciones de desempeño general como “procesamiento aceptable”.	No hay implementación práctica; el modelo es teórico y se limita a la descripción de protocolos y flujos conceptuales.	No se identifican indicadores cuantitativos; el enfoque es cualitativo basado en atributos como identidad y estado en blockchain.

3.1.3.7. Reporte de estudios relacionados con modelos de seguridad por geolocalización

Los estudios revisados demuestran que la geolocalización se ha convertido en un elemento esencial para reforzar la autenticación y detección de fraudes en entornos móviles y bancarios. Modelos como los de Majumdar y Awasthi (2025) y García-

Treviño et al. (2024) lograron una alta efectividad de reducción de falsos positivos a menos del 5 % y precisión del 100 % en radios seguros al integrar IA, IoT y blockchain en la verificación de ubicación. Otros enfoques, como los de Alabdulatif (2023) y Liu (2023), demostraron la capacidad de prevenir ataques y proteger la privacidad con k-anonimato y ocultamiento espacial. En conjunto, los modelos basados en geolocalización fortalecen la autenticación contextual y permiten desarrollar sistemas más seguros, adaptativos y confiables, cuyos resultados en forma detallada se muestra en la tabla 11

Tabla 11
Análisis comparativo de modelos por Geolocalización

Referencia	Descripción del modelo	Arquitectura	Algoritmo	Efectividad	Implementación	Variables/Indicadores
Majumdar y Awasthi (2025)	Integra blockchain, IA e IoT para reforzar la seguridad de sistemas GPS en operaciones de seguridad pública.	Incluye Hyperledger Fabric para blockchain, IA para detección de anomalías y redes IoT para recolección de datos.	Utiliza RNN, CNN y filtros bayesianos para detectar anomalías en trayectorias GPS en tiempo real	Se proyecta una reducción de falsos positivos a menos del 5% y mejora de tiempos de respuesta en un 18%.	Simulada con AnyLogic e integrada en un entorno de cómputo de alto rendimiento (HPC) para escenarios de incendios controlados.	Temperatura, humedad, velocidad del viento, latencia de red, tolerancia a fallos y distancia geoespacial
García-Treviño et al. (2024)	Proponen un algoritmo de autenticación multifactor	Incluye dos implementaciones: una app móvil Android y un sistema	Si el usuario está dentro del radio seguro, accede; si no, se solicita un	Se logró un 100% de precisión en radios seguros de 12 metros	Se probó con 20 usuarios en Android (1165 intentos) y 1	Variables clave: coordenadas GPS, radios de seguridad, tiempos de

	transparente	físico	basado	en	factor de respaldo	(Android) y 30	usuario en Arduino	validación y número de
	basado	en	Arduino	con	como el TOTP.	metros	(739 pruebas).	satélites
	geolocalización	validación		de		(Arduino).		
	como segundo	ubicación.						
	factor.							
Alabdulatif et al. (2023)	Proponen un método de autenticación multifactor basado en geolocalización para proteger transacciones en cajeros automáticos.	Se compone de un cajero automático, la infraestructura bancaria existente y una aplicación móvil que actúa como autenticador.	Se valida la ubicación GPS del usuario contra la ubicación física del cajero automático antes de autorizar la transacción	No se da porcentaje explícito; el sistema declara prevenir skimming, shoulder surfing y spoofing.	Se implementó una simulación con Paragon Virtual ATM y pruebas en entorno controlado usando dispositivos Android.	Variables: ubicación del usuario, ubicación del ATM, límite de retiro, activación de MFA y estado de autenticación.		
Liu et al. (2023)	Desarrollan un esquema de protección de privacidad que combina Geohash, ocultamiento espacial y k-anonimato para consultas de ubicación.	Se basa en un esquema centralizado con usuario, servidor anónimo (AS) y proveedor de servicios de localización (LSP), gestionando datos con GL-Tree.	Aplica dos algoritmos: generación de celdas anónimas y generación de consultas anónimas usando Geohash y medidas de entropía.	El modelo logró una tasa de anonimato del 100% bajo diversas condiciones de prueba.	Se evaluó con el dataset GeoLifeTrajectories 1.3, simulando hasta 500,000 registros de historial de check-ins.	CH (calor de la celda), CQ (frecuencia de consulta), CT (tipo de contenido), similitud semántica y entropía.		

Bartłomiejczyk et al. (2022)	Desarrollan la incorporación de la ubicación como un cuarto factor de autenticación, reforzando los tradicionales: conocimiento, posesión e inherencia.	Consta de una aplicación móvil, una aplicación testigo, un POS y un servicio de autenticación conectados mediante Firebase Cloud Messaging	Opera en dos fases: declaración de ubicación y confianza y confirmación de ubicación mediante firmas digitales de múltiples dispositivos.	No se da un porcentaje exacto, pero se afirma superior a OTP y resistente a ataques MITM y de repetición.	Se creó un prototipo y se realizaron pruebas reales con 200 muestras en red pública para medir tiempos y seguridad.	Variables usadas: identificador de usuario, coordenadas GPS, timestamps, claves criptográficas, ID de sesión y token FCM
Estrela et al. (2021)	Proponen una extensión del marco Biotouch para autenticación continua basada en biometría de dinámica de toque en aplicaciones bancarias.	Se basa en una verificación estática inicial y una verificación dinámica continua, utilizando fusión de puntuaciones (F1 y localización). F1 Score es una métrica de evaluación en aprendizaje automático que combina la precisión y la sensibilidad.	Utiliza Random Forest, SVM, Gradient Boost, XGBoost, Naive Bayes Gaussiano y Bernoulli, seleccionados mediante Grid Search	Se alcanzó un F1 Score de entre 90.68% y 97.05%, con EER de entre 9.85% y 1.88%.	Implementado en la app Android Biotouch, simulando operaciones bancarias reales mediante recopilación de datos de interacción.	Se capturaron entre 29 y 31 variables de interacción, presión, aceleración, rotación, magnetismo y geolocalización

3.2. Análisis y discusiones de la revisión sistemática de la literatura.

3.2.1. Análisis y discusiones de estudios relacionados a los ataques de phishing y smishing.

3.2.1.1. P1: ¿Qué técnicas se han implementado para identificar los ataques de Phishing en la banca móvil sobre dispositivos Android, y cuáles son la precisión, ventajas y limitaciones asociadas a dichas técnicas?

Entre las técnicas más destacadas, los modelos basados en redes neuronales profundas, como CNN, LSTM y Transformers, han mostrado una precisión superior al 95 %, alcanzando en algunos casos valores cercanos al 99 % (Alshingiti et al., 2023; Asiri et al., 2023). Estos enfoques destacan por su capacidad para aprender patrones complejos sin necesidad de ingeniería manual, adaptándose a diversas formas de ataque. No obstante, su alto consumo computacional y dependencia de grandes volúmenes de datos constituyen limitaciones importantes para su implementación en tiempo real.

Por otro lado, los modelos híbridos como BERT + CNN o DAE + AAA + IWO (Elsadig et al., 2022; Alqahtani et al., 2022) han demostrado mejoras en la selección de características y reducción de falsos positivos, aunque requieren hardware especializado y presentan dificultades para escalar en entornos con datos desbalanceados.

Las técnicas tradicionales como Random Forest, RFE y Fuzzy Rule Interpolation (FRI) (Alani y Tawfik, 2022; Almseidin et al., 2022) ofrecen un equilibrio entre precisión y eficiencia, siendo más fáciles de implementar y desplegar en la nube. Sin embargo, su rendimiento depende de la actualización constante de los datos y de la calibración de parámetros.

Otros estudios, como los de Sahingoz et al. (2019) y Sathya et al. (2020), integraron procesamiento de lenguaje natural (NLP) con Random Forest, logrando detección en tiempo real e independencia del idioma, lo que los hace especialmente útiles para entornos móviles multilingües.

En conjunto, los hallazgos evidencian que no existe una técnica única capaz de mitigar completamente los ataques de phishing. Los enfoques más modernos tienden a combinar aprendizaje profundo, procesamiento del lenguaje y modelos híbridos, buscando optimizar la precisión sin sacrificar velocidad ni consumo de recursos. Sin embargo, persiste la necesidad de desarrollar modelos más ligeros, explicables y adaptativos, capaces de responder de manera efectiva ante las nuevas variantes de fraude que evolucionan constantemente en la banca móvil sobre Android.

3.2.1.2. P2: ¿Qué técnicas se han implementado para identificar los ataques de Smishing en la banca móvil sobre dispositivos Android, y cuáles son la precisión, ventajas y limitaciones asociadas a dichas técnicas?

La revisión de la literatura evidencia que el smishing, entendido como el uso de mensajes SMS fraudulentos para engañar a los usuarios y obtener información confidencial, ha impulsado el desarrollo de diversas técnicas de detección basadas en aprendizaje automático y profundo.

Entre las aproximaciones más efectivas se encuentran las que emplean redes neuronales profundas, particularmente CNN y LSTM, las cuales alcanzaron precisiones cercanas al 99 % (Ghourabi et al., 2023; Stevanović, 2022). Estos modelos demostraron gran capacidad para detectar variaciones en el lenguaje y adaptarse a nuevos formatos de mensajes, lo que los hace altamente eficaces para entornos dinámicos como la banca móvil. Sin embargo, su implementación requiere alto poder computacional, grandes volúmenes de datos y una infraestructura compleja, además de presentar cierta vulnerabilidad frente a ataques adversariales que manipulan sutilmente el contenido de los mensajes.

Por otro lado, los enfoques basados en aprendizaje automático supervisado, como XGBoost, Extra Trees, RIPPER y C4.5, han mostrado resultados notables con precisiones que superan el 97 % (Akande et al., 2023; Gualberto et al., 2020; Mambina et al., 2022). Su principal fortaleza radica en su equilibrio entre precisión, interpretabilidad y eficiencia, lo que los convierte en una opción viable para

dispositivos móviles con recursos limitados. No obstante, su rendimiento depende en gran medida de la calidad y el equilibrio del conjunto de datos, pudiendo generar sobreajuste o sesgos cuando las muestras no representan adecuadamente las distintas formas de ataque.

Asimismo, algunos investigadores han explorado métodos no supervisados, como Mean Shift y DBSCAN (Althobaiti et al., 2023), los cuales permiten descubrir nuevos patrones de smishing sin necesidad de datos etiquetados. Aunque su aporte resulta valioso para la detección temprana de campañas desconocidas, presentan una precisión inferior (82 %) y un alto costo computacional, lo que limita su aplicabilidad práctica.

Modelos más recientes, como el FMMPED (Qi et al., 2023), incorporan estrategias de muestreo de Markov para optimizar la detección y reducir falsos positivos, alcanzando una precisión del 97.97 %, mientras que enfoques híbridos, como el de Mishra y Soni (2020), combinan análisis de código fuente, URLs y APK maliciosos, ofreciendo una visión más completa del ecosistema de fraude móvil. En síntesis, los estudios coinciden en que no existe una técnica única capaz de eliminar completamente los ataques de smishing. Las soluciones más exitosas son aquellas que integran modelos híbridos, combinando la potencia del deep learning, la eficiencia de los algoritmos clásicos y el análisis contextual del mensaje. Sin embargo, los desafíos persisten en torno a la dependencia de grandes datasets, la adaptación a nuevas variantes de ataque y la necesidad de modelos más ligeros y explicables que puedan ejecutarse eficazmente en dispositivos Android sin comprometer el rendimiento.

3.2.2. Análisis y discusiones, de estudios relacionados con el fraude informático en las modalidades de Fake Apps y SIM Swapping.

3.2.2.1.P1: ¿Qué técnicas se han implementado para mitigar el fraude informático en la modalidad de Fake App en la banca móvil sobre dispositivos Android, y cuáles son la precisión, ventajas y limitaciones asociadas a dichas técnicas?

Los estudios realizados por Vanjire y Lakshmi (2024) propusieron un enfoque innovador que combina redes neuronales convolucionales (CNN) con sistemas explicables de inteligencia artificial (XAI), logrando más del 99 % de precisión en la detección de aplicaciones falsas. Su principal fortaleza radica en la capacidad de interpretar los resultados, permitiendo a los analistas comprender por qué una aplicación es catalogada como fraudulenta. Sin embargo, el modelo requiere recursos intensivos de GPU, lo que dificulta su implementación en dispositivos móviles de gama media o baja.

Por su parte, Udayakumar et al. (2024) integraron GIST, FFNN y Random Forest, alcanzando un 98 % de efectividad al analizar la estructura interna de los archivos APK y DEX. Aunque su desempeño fue sobresaliente, este modelo depende del acceso completo a los archivos de la aplicación, una condición que limita su uso en sistemas con medidas de seguridad que restringen dicho acceso.

Un enfoque distinto fue presentado por Prayogi y Aji (2023), quienes desarrollaron el método Mobile Network Verification (MNV), basado en la validación de la identidad del usuario a través de su conexión móvil. Este modelo alcanzó un 100 % de detección, demostrando una efectividad total en entornos controlados. No obstante, su aplicabilidad a gran escala depende de políticas gubernamentales y de la cooperación con operadores de red, lo que dificulta su adopción global.

De manera complementaria, Anjum et al. (2022) implementaron Bayesian Neural Networks (BNN), logrando precisiones superiores al 99 %, aunque su complejidad computacional y la necesidad de grandes volúmenes de datos limitan su escalabilidad. En contraste, los modelos de Xie et al. (2021) y Ullah et al. (2021) utilizaron árboles de diseño fusionado (MLT) y gráficos de flujo de control (CFG) combinados con RNN, logrando también buenos resultados, pero con un alto riesgo de falsos positivos y una demanda significativa de procesamiento cuando se aplican a aplicaciones de gran tamaño.

Finalmente, los estudios más tradicionales, como los de Gezer et al. (2019) y Zhang et al. (2019), recurrieron a modelos estadísticos clásicos como Random Tree, Naive Bayes y firmas digitales, con precisiones entre 83 % y 91 %. Aunque su bajo costo computacional

los hace atractivos, resultan insuficientes frente a las sofisticadas técnicas de ofuscación empleadas por los desarrolladores de Fake Apps.

Al comparar estos enfoques con el modelo SectraBank, se observa una diferencia fundamental en la naturaleza de la defensa. Mientras los modelos tradicionales y de IA buscan detectar una Fake App mediante el análisis de su código, comportamiento o estructura, el modelo SectraBank se centra en prevenir el fraude antes de que ocurra, validando de forma simultánea la identidad del usuario (biometría), la autenticidad del dispositivo (IMEI) y la ubicación geográfica (geolocalización). En lugar de depender de grandes conjuntos de datos o del análisis del APK, SectraBank vincula cada transacción con un entorno legítimo y verificable, reduciendo así la probabilidad de ejecución de operaciones fraudulentas incluso si una aplicación falsa logra instalarse.

Mientras que el modelo de Vanjire y Lakshmi (2024) destaca por su precisión explicable, y el de Prayogi y Aji (2023) por su dependencia de la red móvil, SectraBank ofrece una ventaja práctica: no requiere infraestructura externa ni entrenamiento previo, operando directamente sobre el contexto real del usuario. Su principal fortaleza radica en su enfoque preventivo y contextual, aunque también enfrenta desafíos, como la dependencia de señales GPS precisas y la necesidad de una configuración óptima de umbrales de seguridad para evitar falsos rechazos. El modelo SectraBank representa una alternativa complementaria e innovadora, ya que no busca únicamente detectar el fraude, sino evitar que este se concrete, integrando autenticación biométrica, verificación de dispositivo y control geográfico en un mismo ecosistema de seguridad. Esta combinación convierte a SectraBank en un modelo más adaptativo, accesible y aplicable para el entorno bancario Android, donde la protección en tiempo real y la experiencia del usuario resultan esenciales.

3.2.2.2.P2: ¿Qué técnicas se han implementado para mitigar el fraude informático en la modalidad de SIM Swapping en la banca móvil sobre dispositivos Android, y cuáles son la precisión, ventajas y limitaciones asociadas a dichas técnicas?

La literatura reciente converge en un enfoque multicapa que combina verificación del dispositivo, autenticación robusta y contexto de uso. En el extremo de la detección

precisa, Oh et al. (2023) emplean model checking con UPPAAL y device fingerprinting, alcanzando 100% de acierto en pruebas controladas al detectar cambios sospechosos de dispositivo. Su talón de Aquiles es la cobertura del repositorio de huellas: si el fingerprint no representa la diversidad real de terminales, crecen los falsos negativos.

En la capa de autenticación, Kim et al. (2022) proponen MFA con biometría, tokens físicos y blockchain: eleva la seguridad, pero exige infraestructura costosa y operación compleja a gran escala. Hassan y Shukur (2021) demuestran también 100% en su entorno al combinar MFA + RSA + Firebase, aunque dependen de plataformas externas (p. ej., PayPal) y conectividad confiable. Desde el ángulo de IA, Kala (2021) muestra que ANN + Random Forest (94%) permiten detección proactiva de patrones ligados al intercambio ilícito de SIM; no obstante, requieren colaboración con operadores para acceder a señales de red. En clave criptográfica, Kisore y Sagi (2015) (EC-MQV + AES-256) refuerzan autenticaciones de bajo valor, pero siguen expuestas a malware y estaciones base falsas.

De forma transversal, los avances en mitigación de Fake App (hashing TLSH/MinHash, análisis CFG, CNN/RNN) mejoran la integridad del binario y reducen vectores que facilitan el SIM Swapping (p. ej., secuestro de OTP). La tendencia, por tanto, es defensa en profundidad: atestación del dispositivo, MFA, señales de red y análisis inteligente.

Comparación con el modelo SectraBank. SectraBank opera como barrera preventiva y contextual: biometría + IMEI + geolocalización + hora de servidor. A diferencia de los detectores basados en fingerprinting o blockchain, no depende de repositorios externos ni de operadores, y no requiere entrenar modelos pesados.

3.2.2.3.P3: ¿Qué modelos, arquitecturas y algoritmos basados en técnicas de biometría han sido implementados para mitigar el fraude informático en aplicaciones bancarias Android, y cuáles son su efectividad, variables e indicadores de evaluación?

Entre los avances más notables, Awad et al. (2024) desarrollaron un sistema de autenticación multimodal que combina reconocimiento facial y de huellas dactilares dentro de una arquitectura distribuida IoT. Este modelo, basado en redes neuronales

convolucionales (CNN), permitió alcanzar niveles de precisión de entre 93 % y 97 %, mostrando una alta fiabilidad en la verificación del usuario. Sin embargo, su implementación exige procesamiento en la nube y control de tasas de error como el FAR (False Acceptance Rate) y FRR (False Rejection Rate), lo que incrementa la complejidad operativa.

Por su parte, Khan et al. (2023) destacaron el papel de la autenticación multifactor (MFA) en las transacciones móviles, evidenciando que la combinación de factores como OTP, biometría y blockchain puede incrementar la seguridad en un 46 %. Aunque su propuesta fue teórica, demuestra la importancia de integrar múltiples capas de defensa. En la misma línea, Ali et al. (2021) implementaron una arquitectura funcional que une PIN, OTP y biometría bajo un marco criptográfico robusto con algoritmos SHA-256, RSA y FIDO, logrando un equilibrio entre seguridad y eficiencia en entornos financieros reales. Los aportes de Lien y Vhaduri (2023) y Bedari et al. (2022) refuerzan la eficacia del reconocimiento por huellas dactilares. Este último logró tasas de error igualado (EER) inferiores al 1 % gracias al uso de plantillas cancelables sobre redes 5G, garantizando tanto precisión como protección de la información biométrica. A su vez, Bairwa y Joshi (2021) plantearon un enfoque de autenticación mutua, que combina la huella digital con la dirección MAC y tokens de sesión, mejorando la integridad de los nodos y la comunicación entre dispositivos en entornos distribuidos. En conjunto, los estudios coinciden en que la biometría multimodal y los esquemas MFA ofrecen los mejores resultados frente a fraudes en banca móvil. No obstante, las principales limitaciones siguen relacionadas con el alto consumo de recursos, la latencia de red y los desafíos en privacidad y protección de datos biométricos, especialmente cuando se almacenan o procesan en la nube.

Al comparar estos avances con el modelo SectraBank, se observa un enfoque distinto pero complementario. Mientras los modelos tradicionales se centran en verificar la identidad mediante rasgos biométricos, SectraBank incorpora una capa de contextualización al validar simultáneamente la biometría del usuario, el IMEI del dispositivo, la geolocalización y la hora del servidor. Esta integración convierte a SectraBank en un sistema preventivo, capaz de impedir transacciones fraudulentas antes de su ejecución, incluso si el atacante logra suplantar la aplicación o interceptar la SIM.

3.2.2.4.P4: ¿Qué modelos, arquitecturas y algoritmos basados en código IMEI han sido implementados para mitigar el fraude informático en aplicaciones bancarias Android, y cuáles son su efectividad, variables e indicadores de evaluación?

Las soluciones antifraude se apoyan en plataformas móviles (Android Studio, SDK Android) y herramientas de seguridad integradas como BiometricPrompt, TelephonyManager (para IMEI), y APIs de localización GPS (García-Treviño et al., 2024). En esta línea, SAM-PAY (Berbecaru, 2025) propone una defensa “situacional”. No solo verifica al usuario: certifica el lugar. Integra GNSS con un Elemento Local que valida coordenadas y, sobre ellas, deriva dinámicamente la OTP aplicando SHA-256 y operaciones XOR al esquema LDEA. El resultado es una clave que “nace” del dónde y del con qué (dispositivo). Aunque no publica un porcentaje de precisión, el prototipo funcional evidencia factibilidad y buena respuesta en pruebas reales. Sus variables clave IMEI, credenciales, claves compartidas, coordenadas certificadas y OTP orientan los indicadores: latencia de validación, tasa de transacciones autorizadas en zona válida, falsos rechazos por error de georreferenciación y uptime del servicio de localización.

Los estudios propuestos por Zamwallet (Hassan & Shukur, 2022) integra IMEI + huella + contraseña + OTP sobre una arquitectura en nube (Firebase) y pasarela PayPal, protegidas con RSA (2048 bits). Reporta éxito funcional en los flujos (registro, login, recarga, transferencia), útil para banca móvil en producción. Aquí, los indicadores recomendables son FAR/FRR de la biometría nativa, tasa de OTP fallidos, tiempos de login/transferencia y disponibilidad del backend; la limitación es la dependencia de terceros y de conectividad estable. Como propuesta de equilibrio entre seguridad y conveniencia, Zukarnain et al. (2022) definen mobile identity: un servidor de autenticación emite tokens cifrados tras validar IMEI, SIM, huella y GPS. Es un diseño conceptual con ejemplos de código Android/iOS; faltan métricas, pero sus variables/indicadores son claros: tasa de tokens válidos, latencia de emisión/verificación y denegaciones por permisos o falta de señales (IMEI/GPS/biometría). Finalmente, Alsunaidi & Almuhaideb (2021) sitúan el problema en blockchain permissionada: registrar propiedad e identidad del smartphone vía smart contracts. Aporta no repudio y una traza de propiedad, aunque se mantiene.

3.2.2.5.P5: ¿Qué modelos, arquitecturas y algoritmos basados en técnicas de geolocalización han sido implementados para mitigar el fraude informático en aplicaciones bancarias Android, y cuáles son su efectividad, variables e indicadores de evaluación?

Con relación a los modelos de geolocalización, destacan el modelo de Majumdar y Awasthi (2025) que muestran un enfoque de defensa en profundidad: combinan IA + IoT + blockchain para vigilar trayectorias GPS y detectar desviaciones con menos del 5 % de falsos positivos y mejoras de respuesta del 18 %. La cadena de bloques aporta trazabilidad e integridad de eventos, mientras que la IA filtra ruido y camuflaje en tiempo real. Por su parte, García-Treviño et al. (2024) prueban la autenticación transparente por geofencing: si el usuario está dentro del radio seguro, la operación fluye; si no, se activa un factor de respaldo (p. ej., TOTP). En pruebas controladas reportan precisión del 100 % en radios de 12–30 m, lo que sugiere que, con calibración fina, la ubicación puede ser un segundo factor silencioso y muy efectivo.

SectraBank parte de la misma intuición, pero la operacionaliza: biometría + IMEI + geolocalización + hora de servidor. A diferencia de diseños que dependen de operadores o blockchain, SectraBank minimiza dependencias externas y usa la ubicación como factor contextual para autorizar o bloquear, incluso si una Fake App o un atacante controlan el número. Su ventaja es preventiva: no solo detecta, impide la transacción fuera de contexto.

3.2.2.6.P6: ¿Qué se ha reportado sobre la usabilidad y aceptación por parte de los usuarios al implementar medidas de seguridad multicapa?

La aceptación de medidas de seguridad multicapa depende de su transparencia y facilidad de uso (Abi Din et al., 2021; Sharma & Ghosh, 2021). Los usuarios son más receptivos si perciben que las protecciones no interfieren con la experiencia de uso normal. Modelos que integran biometría, IMEI y geolocalización han sido bien valorados en estudios recientes, con tasas de aceptación superiores al 90% (Ikhsan et al., 2024; Estrela et al., 2021). En Sectrabank, los usuarios calificaron la solución como altamente usable y confiable, alcanzando tasas de aceptación de 95-96% en el grupo experimental, confirmando que la seguridad robusta puede coexistir con una experiencia de usuario amigable.

CAPÍTULO 4: METODOLOGÍA PARA LA VALIDACIÓN DEL MODELO

4.1. Hipótesis

4.1.1. Hipótesis general

El modelo Sectrabank mitiga significativamente los incidentes de fraude informático y es percibido positivamente en términos de accesibilidad, usabilidad y aceptación por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

4.1.2. Hipótesis específicas

- a. El modelo Sectrabank permite la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android
- b. El modelo Sectrabank contribuye a la mitigación del fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.
- c. El modelo Sectrabank es percibido como accesible, comprensible y fácil de usar por los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.
- d. El modelo Sectrabank es aceptado por los usuarios como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

4.2. Operacionalización de variables

La identificación y definición precisa de las variables de estudio constituye un componente esencial en el proceso investigativo, ya que orienta la recolección y el análisis de datos de forma coherente con los objetivos planteados (Hernández-Sampieri et al., 2021). En este sentido, a continuación, se presentan los procedimientos técnicos e

indicadores específicos diseñados para operacionalizar y medir las variables que sustentan esta investigación: Mitigación del Fraude Informático en Operaciones Electrónicas a través de Aplicaciones Bancarias en Dispositivos Android (variable dependiente), y el Modelo Sectrabank (variable independiente)

Tabla 12
Operacionalización de la variable dependiente

Variable dependiente	Definición conceptual	Definición operativa	Dimensiones	Indicadores
Mitigación del fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android	Conjunto de estrategias, mecanismos y tecnologías orientadas a mitigar y reducir el fraude informático en operaciones electrónica a través de aplicaciones móviles.	Corresponde a la ocurrencia o intento de fraude informático a través de Fake Apps y SIM Swapping que será mitigado por el modelo Sectrabank.	Mitigación de Fake Apps	Porcentaje de detección de aplicaciones no legítimas. Bloqueo automático de aplicaciones fraudulentas.
			Mitigación de SIM Swapping	Verificación de cambio de SIM (últimas 48h). Consistencia del IMEI.
			Bloqueo de transacciones sospechosas	Número de condiciones anómalas concurrentes (≥ 3). Efectividad del algoritmo de bloqueo.
			Percepción de confiabilidad	Percepción del usuario sobre la seguridad del sistema.

Tabla 13
Operacionalización de la variable independiente

Variable independiente	Definición conceptual	Definición operacional	Dimensiones	Indicadores
Modelo Sectrabank	El Modelo Sectrabank es una arquitectura de seguridad informática desarrollada para aplicaciones bancarias móviles en dispositivos Android., orientados a prevenir ataques de fraude informático, especialmente en las modalidades de Fake App y SIM Swapping.	Desarrollo tecnológico que integra autenticación biométrica, verificación de IMEI, geolocalización, evaluación de permisos, OTP y control de SIM para mitigar el fraude informático	Autenticación biométrica	Tasa de éxito en el reconocimiento de huella dactilar.
			Validación de IMEI y geolocalización	Correspondencia del IMEI y ubicación habitual.
			Evaluación de permisos de la app	Detección de permisos anómalos en la app bancaria.
			Control de OTP y SIM	Frecuencia de OTP múltiples y cambios recientes de SIM.

4.3. Matriz de consistencia

Tabla 14
Matriz de consistencia

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLES	DISEÑO METODOLÓGICO	POBLACION Y MUESTRA
¿Es posible desarrollar un modelo denominado Sectrabank que permita mitigar efectivamente el fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android, mejorando la detección de Fake App y SIM Swapping, así como la aceptación y usabilidad percibida por los usuarios?	Desarrollar el modelo Sectrabank para mitigar efectivamente el fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android, mejorando la detección de Fake App y SIM Swapping, así como la aceptación y usabilidad percibida por los usuarios.	El modelo Sectrabank mitiga significativamente los incidentes de fraude informático y es percibido positivamente en términos de accesibilidad, usabilidad y aceptación por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.	Variable Independiente: Modelo Sectrabank Variable Dependiente: Mitigación del Fraude Informático en Operaciones Electrónicas a través de Aplicaciones Bancarias en Dispositivos Android	Enfoque: Cuantitativo Diseño: Experimental Tipo de Investigación: Aplicada – transversal Nivel de Investigación: Explicativo Método de investigación: Hipotético deductivo	Población • Estudiantes del décimo ciclo de Ingeniería de Software (UNMSM) • Especialistas de la DIVINDAT Muestra: 160 usuarios Instrumento: Encuesta
PROBLEMAS ESPECÍFICO	OBJETIVOS ESPECÍFICOS	HIPÓTESIS ESPECÍFICAS			
PE1: ¿Cómo debe desarrollarse un modelo denominado Sectrabank que permita la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android?	OE1: Desarrollar un modelo denominado Sectrabank que permita la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.	HE1: El modelo Sectrabank permite la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.			

PE2: ¿Qué mecanismos deben integrarse en el desarrollo del modelo Sectrabank para mitigar el fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android?	OE2: Integrar mecanismos funcionales y tecnológicos en el modelo Sectrabank que permitan mitigar el fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.	HE2: El modelo Sectrabank contribuye a la mitigación del fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.
PE3: ¿Qué características deben ser consideradas en el desarrollo del modelo Sectrabank para garantizar que sea percibido adecuadamente en términos de accesibilidad, comprensión y facilidad de uso por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android?	OE3: Incorporar características de accesibilidad, comprensión y facilidad de uso en el modelo Sectrabank, considerando las necesidades de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.	HE3: El modelo Sectrabank es percibido como accesible, comprensible y fácil de usar por los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.
PE4: ¿Qué criterios deben ser contemplados en el desarrollo del modelo Sectrabank para validar la aceptación por parte de los usuarios en términos de confiabilidad, eficacia y adaptabilidad en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android?	OE4: Establecer criterios de confiabilidad, eficacia y adaptabilidad en el desarrollo del modelo Sectrabank que favorezcan su aceptación por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.	HE4: El modelo Sectrabank es aceptado por los usuarios como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

4.4. Tipo y diseño de investigación

Según Lafuente y Egoscozábal (2008), la metodología general de la investigación se fundamenta en el método científico, el cual integra un conjunto de estrategias para la generación de conocimiento. Este proceso se distingue por la aplicación de diversos enfoques, incluyendo el deductivo, inductivo, empírico y científico.

El presente estudio se clasifica como una investigación aplicada, ya que el diseño y desarrollo del modelo Sectrabank tiene como propósito mejorar la seguridad en las operaciones electrónicas, utilizando el conocimiento para resolver problemas específicos (Cordero, 2009). Este enfoque permite realizar pruebas de soluciones en entornos reales o simulados y establecer relaciones entre diferentes variables, evaluando la aparición de ciertos fenómenos. De este modo, el estudio busca desarrollar problemas e hipótesis que conduzcan a una comprensión más detallada y explicativa de los temas abordados. Estas hipótesis facilitan el planteamiento de problemas que orientan la investigación hacia la formulación de nuevas hipótesis y conocimientos (Hernández Sampieri et al., 2021; Medina et al., 2023).

Asimismo, esta investigación sigue un diseño experimental, sustentado en los postulados de (Kerlinger & Lee, 2002), quienes establecen que la investigación experimental se caracteriza por el control de variables externas, la aleatorización de los sujetos o unidades de estudio y el uso de grupos de control y experimentales para medir los efectos de la manipulación de variables. Este diseño es común en estudios de ciencias naturales y sociales, incluyendo investigaciones en ciberseguridad.

El alcance del estudio es explicativo, ya que examina la realidad de las circunstancias en cuestión con el propósito de ilustrar y clarificar una interpretación estructurada y precisa, facilitando un análisis comprensible para el lector (Hernández Sampieri et al., 2021; Medina et al., 2023).

En esta investigación, las variables fueron manipuladas de manera intencionada con el objetivo de observar los problemas en su contexto natural y proceder a su análisis posterior. El enfoque adoptado es cuantitativo, centrado en atributos y propiedades medibles que describen y explican con precisión los fenómenos observados, tanto en grupos sociales como en individuos. Se recurrió a la recopilación de datos, observación y

representación de fenómenos, con un énfasis especial en la cuantificación. En este sentido, las preguntas e hipótesis emergieron a lo largo del proceso de investigación y no necesariamente desde su inicio (Hernández Sampieri et al., 2021; Baena Paz, 2017).

4.5. Alcance del estudio

El alcance del estudio se delimita a una muestra representativa de 160 expertos, conformada por estudiantes de últimos ciclos de la Escuela Profesional de Ingeniería de Software de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos (UNMSM) y especialistas en delitos informáticos adscritos a la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), quienes constituyen la población objetivo para el análisis y validación del modelo Sectrabank.

4.6. Población y muestra

4.6.1. Características de la población y muestra

La población y muestra de este estudio estuvo conformada por dos grupos específicos, seleccionados para participar en la prueba experimental del modelo Sectrabank. Estos grupos intervinieron en un entorno controlado, diseñado para evaluar el desempeño y la efectividad del modelo propuesto:

- 1. Estudiantes de últimos ciclos de la Escuela Profesional de Ingeniería de Software de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos (UNMSM):**

Incluye estudiantes con formación en ingeniería de software y competencias técnicas en el desarrollo y análisis de sistemas informáticos, con conocimientos en la temática de la ciberseguridad. Este grupo, conformado por entre 80 estudiantes, aporta una perspectiva académica y técnica para evaluar el modelo Sectrabank en dispositivos móviles con sistema Android. La información fue obtenida a través de una comunicación vía correo electrónico, en respuesta a la solicitud formal realizada a la Universidad Nacional Mayor de San Marcos, se obtiene la cantidad de alumnos matriculados en el décimo ciclo de la carrera de Ingeniería de Software, conforme se evidencia en el Anexo

10, titulado: *Constancia de cantidad de alumnos matriculados en décimo ciclo de Ingeniería de Software de la UNMSM.*

2. Especialistas de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT):

Compuesto por 80 profesionales capacitados en ciberseguridad con experiencia en la investigación de delitos informáticos, conforme se especifica en el DS 10-2018-JUS "Protocolos de actuación interinstitucional específicos para la aplicación del Código Procesal Penal Peruano", donde se especifica que la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) tiene como función: "1. Investigar y denunciar los delitos informáticos; y aquellos cometidos mediante el uso de la Tecnología de la Información y Comunicaciones (TICs), cuando en la comisión de los hechos se evidencie la participación de integrantes de una organización criminal y 2. Brindar apoyo técnico a las Sub Unidades del SINCRÍ, en la investigación de los delitos donde se emplee los TICs.". Por lo antes expuesto, el conocimiento práctico en ciberseguridad e investigación del cibercrimen complementa el análisis técnico del modelo Sectrabank en dispositivos móviles con sistema Android. La información fue proporcionada por la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la DIRINCRI – PNP, conforme se evidencia en el Anexo 9, titulado: *Constancia de cantidad de efectivos policiales encargados de investigar delitos informáticos.*

4.6.2. Tamaño de muestra

Se seleccionó a 80 encuestados de los estudiantes de la Escuela Profesional de Ingeniería de Software y a los 80 integrantes de la DIVINDAT, considerando que todos los participantes de ambos grupos utilizan dispositivos móviles Android. Dado que la población total es relativamente pequeña (160 personas), el estudio abarca de manera adecuada a la totalidad de la población como muestra, lo que garantiza un margen de error mínimo y asegura la representatividad de los resultados. Este enfoque permite una recolección de datos precisos mediante herramientas digitales optimizadas para Android, sin que esto afecte la validez del estudio.

4.6.3. Selección de muestra

La muestra utilizada en este estudio estuvo conformada por 160 participantes, seleccionados bajo criterios específicos alineados con los objetivos de la investigación. Se aplicó un muestreo no probabilístico de tipo intencional o por conveniencia, dado que los participantes fueron escogidos considerando características particulares relevantes para el fenómeno en estudio, tal como lo señalan Grobler et al. (2021). Asimismo, Hernández-Sampieri et al. (2021) afirman que, cuando la población es relativamente pequeña y accesible, resulta factible aplicar un censo, lo cual permite analizar a todos los elementos sin recurrir a técnicas de muestreo. De manera concordante, Babbie (2010) indica que un censo es pertinente cuando se puede examinar a la totalidad de los miembros de una población claramente delimitada y manejable. En este sentido, el tamaño y accesibilidad de la población en esta investigación permitieron incorporar a todos sus integrantes, lo que garantiza una representatividad adecuada de los datos y minimiza el margen de error muestral. El tamaño de la muestra fue determinado tras la aplicación de una encuesta, la cual se implementó mediante un formulario que se presenta en el Anexo 3, titulado: *Formulario para las personas que usaron el Modelo Sectrabank*. Dicho instrumento fue elaborado considerando tres criterios fundamentales:

- **Pertinencia temática:** Los participantes fueron seleccionados por su conocimiento y experiencia en áreas relevantes, como la seguridad informática y el uso de aplicaciones bancarias en dispositivos Android.
- **Factores de seguridad:** Dada la sensibilidad del tema, relacionado con vulnerabilidades en la seguridad bancaria, se optó por trabajar con una muestra No limitada para garantizar la confidencialidad y protección de los datos.
- **Acceso y control:** La muestra pequeña permitió realizar un análisis más controlado y profundo en las simulaciones de ataques (Fake App y SIM Swapping), asegurando la calidad de los datos obtenidos.

4.7. Desarrollo de la investigación

La metodología experimental del modelo Sectrabank se enfoca en evaluar la efectividad de medidas de seguridad para mitigar los ataques fraude informático en las

modalidades de Fake App y SIM Swapping. El estudio se estructura mediante pruebas controladas a través de dos grupos: control y experimental. El grupo de control utiliza la aplicación bancaria estándar, sin contar con las medidas de seguridad. El grupo experimental emplea el modelo Sectrabank con la implementación de las tres capas de seguridad. Los participantes son seleccionados aleatoriamente y las variables clave incluyen la incidencia de ataques y la efectividad de las contramedidas implementadas. El objetivo es determinar la superioridad del modelo Sectrabank en la protección de los usuarios frente a estos tipos de amenazas.

CAPÍTULO 5: PROPUESTA DEL MODELO SECTRABANK

El presente capítulo desarrolla el modelo propuesto denominado Sectrabank, el cual constituye el aporte central de esta investigación. Sectrabank ha sido desarrollado como una solución integral de seguridad para mitigar el fraude informático en operaciones bancarias a través de dispositivos Android, abordando especialmente las modalidades de Fake App y SIM Swapping. Este modelo se fundamenta en una arquitectura de seguridad multicapa que integra la validación del IMEI, la geolocalización en tiempo real y la autenticación biométrica, con el fin de prevenir el acceso no autorizado y fortalecer la confianza del usuario. El modelo SectraBank ha sido desarrollado tomando como base conceptual el estudio de Zukarnain et al. (2022), quienes plantean un esquema de autenticación móvil que combina biometría, identificación del dispositivo y geolocalización para fortalecer la seguridad frente a fraudes. Dicho enfoque ha servido como sustento teórico para integrar mecanismos como la validación del IMEI, la autenticación por huella dactilar y la verificación de ubicación en la propuesta de esta investigación. La construcción del modelo responde a un análisis independiente de patrones ciber criminales, adaptando y extendiendo los principios identificados en la literatura para abordar específicamente los riesgos de Fake App y SIM Swapping en banca móvil, tal como se ilustra en la figura 8.

5.1. Fundamentos del Modelo Sectrabank

La propuesta del modelo Sectrabank surge como alternativa frente a los métodos tradicionales de mitigación del fraude, como la autenticación vía OTP (Token digital), que pueden ser vulnerados mediante SIM Swapping, así como el Fake Apps utilizadas para controlar los dispositivos móviles de forma remota y capturar credenciales críticas como la clave OTP. Por ello, Sectrabank se desarrolla bajo fundamentos técnicos que integran múltiples mecanismos de verificación y detección, operando en tiempo real.

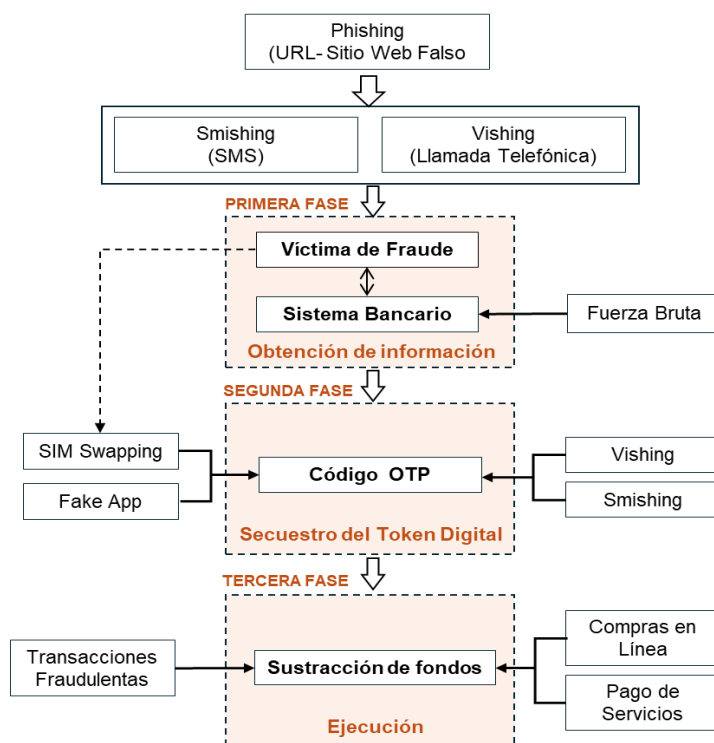
El modelo Sectrabank, se alinea con principios teóricos como la Teoría de la Seguridad de la Información (Whitman y Mattord, 2017), que enfatiza la confidencialidad, integridad y disponibilidad; la Teoría de la Gestión de Riesgos (Hansford y Peltier, 2018), que permite identificar vulnerabilidades; y la Teoría de la

Gestión de Amenazas Integradas (McBride, 2008), que respalda la unificación de múltiples capas de seguridad.

5.2. Proceso del fraude

El modelo para mitigar ataques de fraude informático en la modalidad de Fake App y SIM Swapping en teléfonos celulares Android, se concibe tras un análisis exhaustivo del comportamiento cibercriminal de los atacantes. Estos delincuentes logran evadir las medidas de seguridad establecidas para llevar a cabo operaciones bancarias fraudulentas y alcanzar sus objetivos ilícitos, como se ilustra la Figura 9.

Figura 9
Estructura del proceso del fraude



- En la primera fase, el cibercriminal accede a información sensible de la víctima, como los datos de su tarjeta bancaria y el número de teléfono asociado a sus cuentas. Esta información puede ser obtenida mediante técnicas de ingeniería social como el phishing y sus variantes, o, en algunos casos, mediante ataques de fuerza bruta.

- Durante la segunda fase, el atacante emplea métodos de intercambio de SIM y la creación o distribución de aplicaciones maliciosas (Fake Apps) para interceptar el código de verificación de un solo uso (OTP) enviado al dispositivo móvil de la víctima. Esta etapa es crucial, debido a que permite al atacante superar los mecanismos de autenticación de dos factores implementados por las instituciones financieras.
- Finalmente, en la tercera fase, el atacante utiliza la información obtenida y el acceso a la cuenta de la víctima para realizar transacciones fraudulentas. Estas acciones pueden incluir transferencias bancarias no autorizadas, compras en línea o el pago ilícito de servicios. El modelo Sectrabank está diseñado específicamente para interrumpir este ciclo, previniendo la materialización de dichas actividades fraudulentas.

5.3. Diseño del modelo Sectrabank

El Modelo Sectrabank está compuesto por tres capas de seguridad, cada una diseñada para mitigar distintos tipos de ataques informáticos, como el **Fake App** y el **SIM Swapping**, que son particularmente frecuentes en el ámbito de las transacciones electrónicas.

1. Primera capa de seguridad

La primera capa valida las credenciales del usuario mediante el número de cuenta, la contraseña y el código IMEI del dispositivo móvil. Esta información es comparada con los datos almacenados en el servidor de la institución financiera para verificar la identidad del usuario.

2. Segunda capa de seguridad

La segunda capa introduce una validación biométrica mediante la huella dactilar del usuario. En caso de no ser validada, se solicita que el usuario reingrese sus credenciales. Si la validación falla en tres intentos consecutivos, la aplicación es bloqueada, lo que refuerza la protección contra accesos no autorizados.

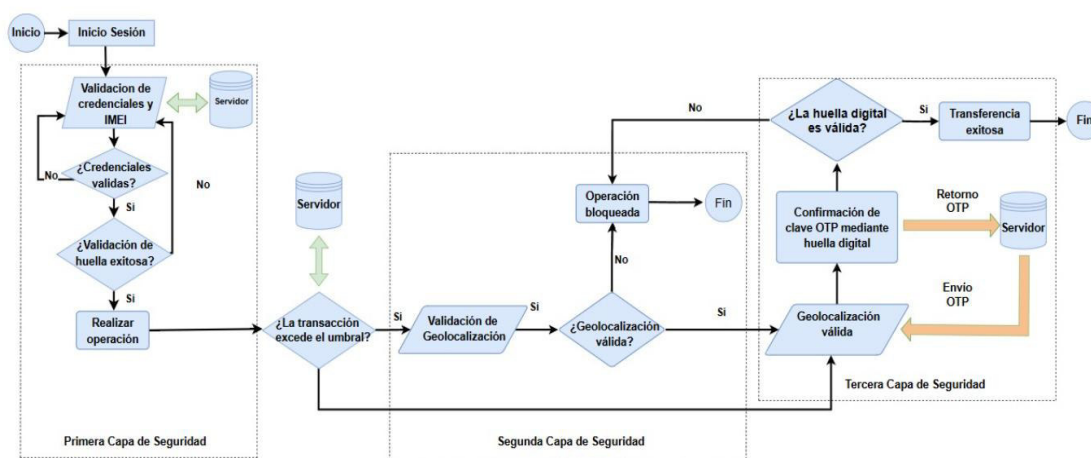
3. Tercera capa de seguridad

La última capa de seguridad se enfoca en la **geolocalización**. El usuario tiene la

posibilidad de designar hasta tres ubicaciones frecuentes para realizar transacciones de alto valor, previamente acordadas con la institución financiera. Para completar una transacción fuera de estas zonas seguras, se requiere que el usuario se encuentre dentro de una zona geográficamente delimitada por una geomalla. Si el usuario intenta realizar una transacción fuera de estas zonas seguras, la operación es automáticamente cancelada.

Adicionalmente, como medida de seguridad, la **validación de la clave OTP** se realiza mediante la verificación de la huella dactilar; lo que garantiza que la autenticación se realiza solo por el usuario legítimo. En la Figura 10 se muestra el flujo de acción de las capas de seguridad del modelo Sectrabank. Por motivos de confidencialidad, únicamente se han incluido fragmentos representativos del código utilizado para el diseño y desarrollo del modelo Sectrabank, los cuales se presentan en las Figuras 12 al 15. Asimismo, el diseño de la interfaz de usuario (UI) con las medidas de seguridad desarrolladas para mitigar ataques de Fake App y SIM Swapping se ilustra en las Figuras 17, 18 y 19. Este conjunto de figuras permite visualizar tanto la estructura funcional del modelo como las estrategias de seguridad aplicadas en la interfaz.

Figura 10
Proceso de las capas de seguridad



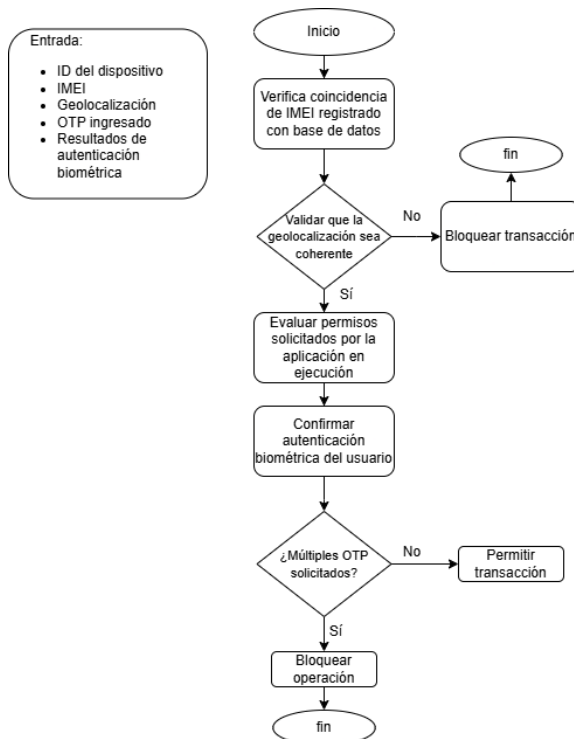
5.4. Algoritmo de seguridad multicapa del modelo Sectrabank

El algoritmo de mitigación de fraude propuesto con el modelo Sectrabank se basa en la evaluación secuencial de múltiples parámetros de seguridad para autorizar o

bloquear una transacción bancaria en dispositivos Android. Este flujo lógico inicia con la recopilación de datos críticos como el ID del dispositivo, IMEI, ubicación geográfica, OTP ingresado y resultado de la autenticación biométrica. A continuación, se ejecutan las siguientes verificaciones, cuyo proceso se representa en la Figura 11:

1. Verificación de IMEI: Se compara el IMEI actual del dispositivo con el previamente registrado en la base de datos del usuario.
2. Validación de geolocalización: Se evalúa si la ubicación del dispositivo es coherente con el historial geográfico habitual del usuario.
3. Evaluación de permisos de la aplicación: Se analizan los permisos que la aplicación en ejecución solicita, detectando accesos no justificados que puedan sugerir una Fake App.
4. Autenticación biométrica: Se valida la identidad del usuario mediante mecanismos biométricos (huella, rostro).
5. Detección de cambio reciente de SIM: Se verifica si el SIM ha sido reemplazado en un periodo inferior a 48 horas.
6. Análisis de múltiples solicitudes de OTP: Se identifica si se han realizado varios intentos de autenticación en corto tiempo, lo cual puede indicar un ataque automatizado o de fuerza bruta.

Figura 11
Diagrama de flujo del Algoritmo de Seguridad Multicapa



5.5. Código fuente del Modelo Sectrabank

El código fuente del Modelo Sectrabank ha sido desarrollado en el lenguaje de programación Java, utilizando el framework Spring Boot y MySQL como base de datos para la gestión del backend. Para la parte del frontend, se ha empleado Kotlin, lo que ha permitido crear una aplicación robusta y eficiente orientada a mitigar los ataques de fraude informático.

Este enfoque técnico ha sido clave para garantizar la seguridad y la efectividad del sistema en la prevención de fraudes en transacciones electrónicas. Debido a la naturaleza confidencial del código fuente, solo se presentará una porción para mantener la confidencialidad del código en el desarrollo de soluciones de ciberseguridad. A continuación, se detalla las porciones del código.

5.5.1. Habilitación de permisos.

En la aplicación Android se implementó el método `FusedLocationProviderClient`, un proveedor de permisos. Este método requiere la

obtención de permisos específicos en el sistema Android, tales como ACCESS_FINE_LOCATION y ACCESS_COARSE_LOCATION, los cuales habilitan el acceso a la ubicación precisa y aproximada del dispositivo, respectivamente. Además, se incluyen permisos adicionales como READ_PHONE_STATE, que permite consultar del teléfono, y USE_FINGERPRINT, utilizado para la autenticación biométrica, estos permisos se pueden observar en la Figura 12.

Figura 12
Permisos necesarios para el desarrollo de la aplicación

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools">

    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.READ_PHONE_NUMBERS" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.READ_PRIVILEGED_PHONE_STATE" />
    <uses-permission android:name="android.permission.READ_PRIVILEGED_PHONE_STATEx" />
    <uses-permission android:name="android.permission.USE_FINGERPRINT" />
```

5.5.2. Huella digital.

Para la autenticación biométrica mediante huella digital, la implementamos en la función setOnClickListener(), esta capta la huella cuando se crea una nueva cuenta en el componente tvCreateAccount. El código verifica la compatibilidad del dispositivo con el sensor de huellas digitales y, si es compatible, configura un objeto Cipher y un CryptoObject para la autenticación. Se muestra un FingerprintDialogFragment que maneja el proceso de autenticación, invocando startAuthentication() para comenzar el proceso. En caso de que el dispositivo no tenga un sensor de huella o no haya huellas registradas, se muestra un diálogo de confirmación al usuario indicando que se requiere un sensor de huella digital para proceder. Este enfoque asegura que la autenticación se realice de manera segura y que se manejen adecuadamente las excepciones relacionadas con la disponibilidad del hardware biométrico, conforme se muestra en la Figura 13.

Figura 13
Código de la Huella Digital

```
private fun setOnClickListener() {
    binding.tvCreateAccount.setOnClickListener {
        val intent = Intent(this@Login, RegisterAccount::class.java)
        startActivity(intent)
        //overridePendingTransition(android.R.anim.fade_in, android.R.anim.fade_out)
    }

    binding.btnLogin.setOnClickListener {
        binding.btnLogin.isEnabled = false
        keyguardManager = getSystemService(Context.KEYGUARD_SERVICE) as KeyguardManager
        fingerprintManager = getSystemService(Context.FINGERPRINT_SERVICE) as FingerprintManager

        with(UtilsShared){
            if (checkFingerprintCompatibility(this@Login,fingerprintManager,keyguardManager)) {
                val keyGenerator = getKeyGenerator()
                val cipher = getCipher(keyGenerator)
                val cryptoObject = FingerprintManager.CryptoObject(cipher)
                val authenticationCallback = MyAuthenticationCallback(this@Login,this@Login)

                fingerprintDialog = FingerprintDialogFragment.newInstance(cryptoObject, authenticationCallback,this@Login)
                fingerprintDialog.show(supportFragmentManager, FingerprintDialogFragment.TAG)

                fingerprintDialog.startAuthentication(cipher, fingerprintManager)
            }
        }
    }
}
```

5.5.3. Ubicación.

Para el manejo de la ubicación creamos una función `requestLocation()`. La función `request Location()` se encarga de obtener la ubicación actual del dispositivo mediante `FusedLocationProviderClient`, que facilita el acceso eficiente a los datos de ubicación. Utilizando el método `lastLocation`, que recupera la última ubicación conocida, esta se empleada en diversas funcionalidades de la aplicación. La respuesta se maneja de forma asíncrona con `addOnSuccessListener`, formateando las coordenadas de latitud y longitud con 8 decimales si la ubicación es válida. Si no se puede obtener la ubicación, se notifica al usuario con un mensaje emergente, asegurando un manejo robusto de la disponibilidad y precisión de los datos de ubicación, conforme se muestra en la figura 14.

Figura 14
Código para obtener la ubicación

```

287     @SuppressWarnings("MissingPermission")
288     private fun requestLocation() {
289
290         fusedLocationClient.lastLocation
291             .addOnSuccessListener { location: Location? ->
292                 location?.let {
293                     latitude = String.format("%.8f", location.latitude)
294                     longitude = String.format("%.8f", location.longitude)
295
296                     //latitude = location.latitude
297                     //longitude = location.longitude
298
299                 } ?: run {
300                     Toast.makeText(this, "Ubicación no disponible", Toast.LENGTH_SHORT).show()
301                 }
302             }
303     }

```

5.5.4. IMEI.

La función `getDeviceId()` obtiene el identificador único del dispositivo, conocido como IMEI, en Android. Primero, verifica si la aplicación tiene el permiso `READ_PHONE_STATE` y, de no ser así, lo solicita al usuario. Una vez concedido el permiso, accede al servicio de telecomunicaciones del sistema a través de `TelephonyManager`. Dependiendo de la versión de Android, utiliza `getImei()` para Android Oreo (API 26) y versiones posteriores, o `getDeviceId()` para versiones anteriores, asegurando así la compatibilidad. Este método permite recuperar el IMEI de forma segura, cumpliendo con las normativas de permisos y privacidad, lo cual es crucial para operaciones que requieren alta autenticación o gestión de dispositivos, conforme se muestra en la Figura 15.

Figura 15
Código del IMEI

```

private fun getDeviceId(context: Context): String{
    if (checkAndRequestPermission(context, android.Manifest.permission.READ_PHONE_STATE,requestCode)) {
        // Si no se tienen los permisos, solicítalos
        ActivityCompat.requestPermissions(this, arrayOf(android.Manifest.permission.READ_PHONE_STATE), 1)
        return ""
    }
    val telephonyManager = context.getSystemService(TELEPHONY_SERVICE) as TelephonyManager

    if (Build.VERSION.SDK_INT >= Build.VERSION_CODES.O) {
        return telephonyManager.imei ?: ""
    } else {
        // Antes de Android Oreo, puedes obtener el IMEI de la siguiente manera
        return telephonyManager.deviceId ?: ""
    }
}

```

5.5.5. Mensaje OTP.

La función `generateTokenDigits` tiene como objetivo producir una cadena de caracteres que contiene una secuencia de dígitos aleatorios, cuya longitud es determinada por el parámetro `length`. Esta función la utilizamos para simular los mensajes OTP (Figura 16), que son mensajes requeridos para autorizar pagos o transferencias de dinero. Este proceso asegura que solo el titular de la cuenta, que tiene acceso al OTP, pueda completar la transacción.

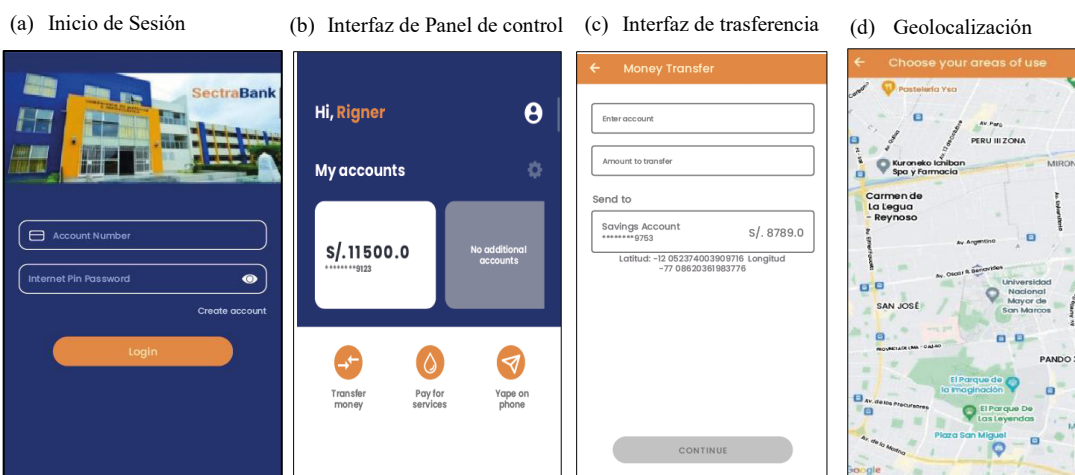
Figura 16
Código Mensaje OTP

```
fun generateTokenDigits(length: Int): String {  
    val random = java.util.Random()  
    val stringBuilder = StringBuilder(length)  
  
    repeat(length) {  
        val digit = random.nextInt(10)  
        stringBuilder.append(digit)  
    }  
  
    return stringBuilder.toString()  
}
```

5.6. Simulación de uso del Modelo Sectrabank

La incidencia de los ataques por las operaciones por móvil motiva el diseño del modelo Sectrabank para la plataforma Android. La integración de las tres capas del modelo Sectrabank presenta cuatro interfaces de usuario, conforme se muestran en la **Figuras 17**, son: **a)** Interfaz de inicio de sesión, **b)** Interfaz de panel de control, **c)** Interfaz de transferencia y **d)** Interfaz de geolocalización.

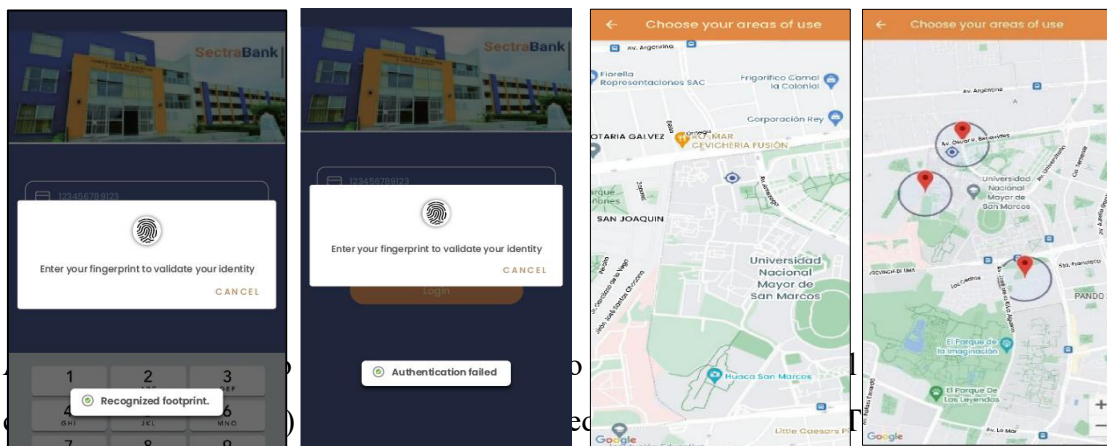
Figura 17
Interfaces de usuario de la aplicación Sectrabank



A continuación, se describe el funcionamiento de las tres capas de seguridad del modelo. En la primera, el inicio de sesión se realiza únicamente validando credenciales correctas, como el IMEI registrado y la huella digital; si son válidas, se muestra un mensaje de autenticación exitosa (Figura 18a). En caso contrario, se deniega el acceso y se muestra un mensaje de error (Figura 18b), lo que contribuye a mitigar el SIM Swapping. La tercera capa, ilustrada en las Figuras 18c y 18d, permite al usuario definir tres puntos geográficos para validar operaciones que superen un umbral de saldo, determinado junto con la entidad bancaria. Si una solicitud de transferencia proviene de una ubicación fuera de esta geomalla, se invalida automáticamente, mitigando así fraudes en la modalidad de Fake App.

Figura 18
Primera, Segunda y Tercera capa de seguridad

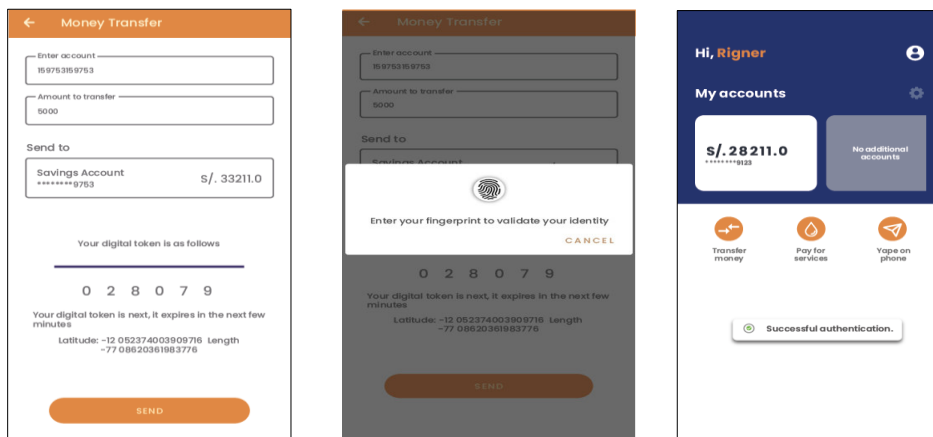
- (a) Autenticación exitosa (b) Autenticación fallida (c) Detección del lugar (d) Puntos de Geomalla



muestra en la Figura 19 (a). La confirmación final de la operación requiere la validación de la huella digital, ilustrada en la Figura 19 (b). Una vez completado este proceso, se emite un mensaje de confirmación de la transferencia

Figura 19
Operación final

- (a) Mensaje OTP (b) Validación de huella Dactilar (c) Transacción exitosa



CAPÍTULO 6: VALIDACIÓN, RESULTADOS Y DISCUSIÓN

6.1. Validación del modelo Sectrabank

6.1.1. Selección de participantes

Se seleccionaron 160 participantes entre estudiantes de Ingeniería de Software de la Universidad Nacional Mayor de San Marcos y Personal Policial, encargados de investigar el cibercrimen, pertenecientes a la DIVINDAT. Siendo el requisito principal el uso de teléfonos celulares con sistema operativo Android. Los policías seleccionados son los encargados de investigar el cibercrimen por su conocimiento especializado respecto a las modalidades de ataques de fraude informático de Fake App y SIM Swapping. Ellos investigan los delitos de fraude informático en sus diferentes modalidades de ataques. Por tanto, ellos, por su conocimiento; reemplazarían a expertos en ciberseguridad.

De ese universo de participantes, son seleccionados 80 como grupo de control, quienes instalaron el modelo Sectrabank sin contar con las medidas de seguridad. Los otros 80 forman el grupo experimental, que utilizan la aplicación bancaria con las medidas de seguridad del modelo Sectrabank implementado que son el Código IMEI, la Huella Dactilar y la Geolocalización.

6.1.2. Experimento

El experimento se realiza en tres fases: Configuración inicial, implementación del modelo, y simulación de ataques.

FASE 1: CONFIGURACIÓN INICIAL

En esta fase, se ha buscado que el Grupo de Control y el Grupo Experimental, tienen perfiles similares en términos de demografía y uso de la tecnología; para lo cual se ha tomado en consideración la edad, género, nivel educativo, ocupación y uso de la tecnología. El criterio de selección ha sido realizado tomando en consideración lo siguiente:

- Edades similares que varía entre 24 a 50 años (Estudiantes de últimos ciclos y efectivos Policiales)

- En cada grupo se ha tomado en consideración igual número de varones y mujeres
- Se ha tomado en consideración igual número de estudiantes universitarios y policías encargados de investigar el cibercrimen.
- Se ha emparejado el uso de tecnología en términos de tipos de aplicaciones y frecuencia de uso.

Asimismo, a ambos grupos se les hizo conocer el funcionamiento de la aplicación Sectrabank, mediante charlas informativas, así como también las modalidades de ataques de fraude informático como Fake App y SIM Swapping.

FASE 2: IMPLEMENTACIÓN DEL MODELO

En la presente investigación, la implementación del Modelo Sectrabank se realizó, mediante un experimento con dos grupos: un grupo de control con medidas de seguridad tradicionales y un grupo experimental con la implementación de los tres niveles de seguridad del modelo, cuyo experimento se ha realizado teniendo en consideración estudios previos sobre interacción humano-máquina, como el de Ciechanowski et al. (2019), el cual permite analizar el impacto de la percepción y respuesta de los usuarios ante interfaces de seguridad en entornos bancarios digitales.

- **Grupo de Control:** Se ha proporcionado el modelo Sectrabank, sin las medidas de seguridad adicionales.
- **Grupo Experimental:** Proporciona la aplicación bancaria con el modelo Sectrabank implementado con las medidas de seguridad que son el Código IMEI, la Huella Dactilar y la Geolocalización

FASE 3: SIMULACIÓN DE ATAQUES

- **Fake App:** Se ha informado a los participantes de ambos grupos sobre la importancia de las medidas de seguridad, así como las técnicas de ataques de Fake App y, con el consentimiento voluntario de los participantes. Se ha simulado el ataque de Fake App, generando accesos remotos al teléfono celular con la finalidad de controlar el teléfono celular y simular transferencias bancarias desde el modelo Sectrabank, cuyos ataques han sido realizados para ambos grupos; es decir, para el Grupo de Control y el Grupo Experimental.

- **SIM Swapping:** Se ha informado a los participantes de ambos grupos sobre la importancia de las medidas de seguridad, así como las técnicas de ataque de SIM Swapping y, con el consentimiento voluntario de los participantes, se ha simulado el ataque de Sim Swapping y se ha realizado transferencias simuladas desde los teléfonos celulares de los participantes seleccionado como Grupo de Control y el Grupo Experimental.

Luego de realizadas estas experiencias, se recogieron los resultados que permitieron conocer cuántos usuarios del grupo de control y del grupo experimental han sido vulnerados.

6.1.3. Técnicas de recolección de datos

La recolección de datos se llevó a cabo mediante la simulación controlada de ataques a dispositivos móviles de los participantes, con el consentimiento informado de cada uno. Para cada escenario se registraron variables como la tasa de éxito del ataque, los tiempos de respuesta del modelo y la percepción de seguridad de los usuarios. Estos datos se analizaron estadísticamente para validar la efectividad del modelo Sectrabank frente a las amenazas de Fake App y Sim Swapping simuladas. El formulario utilizado para la recolección de datos fue validado por un panel de expertos. En el área de ciberseguridad participaron el Ing. Marco Remigio Pusda Chulde, Doctor en Ciencias Informáticas, y el Ing. Diego Miguel Marcillo Parra, Doctor en Tecnologías de la Información y sus Aplicaciones. Del mismo modo, en lo referente a terminología vinculada a las Tecnologías de la Información y la Comunicación (TIC), intervinieron el Ing. Frank Edmundo Escobedo Bailón, Doctor en Ingeniería de Sistemas, Educación y Psicología; el Ing. Luis Antonio Rivera Escriba, Doctor en Ciencias de la Computación; y el Ing. Cayo Víctor León Fernández, Doctor en Ingeniería Informática y de Sistemas. Finalmente, la revisión metodológica y de redacción estuvo a cargo del Ing. Luis Alberto Vives Garnique, Doctor en Educación. Este proceso de validación se encuentra documentado en el Anexo 7, titulado: Actas de validación de herramientas de recopilación de datos. Las respuestas obtenidas mediante dicho formulario se presentan en el Anexo 4, titulado: Respuestas recopiladas *en el formulario*, correspondientes tanto al A) Grupo de Control como al B) Grupo Experimental. Asimismo, se realizaron registros

fotográficos durante la aplicación de la prueba del aplicativo por parte de efectivos policiales, los cuales se muestran en el Anexo 8, titulado: *Imágenes de encuestas a la DIVINDAT*.

6.2. Pruebas de hipótesis

6.2.1. Prueba de normalidad

Teniendo en cuenta que el tamaño de la muestra supera los 50 participantes, se empleó la prueba de Kolmogórov–Smirnov, tal como lo sugiere Saldaña (2016) y lo respaldan González-Estrada y Cosmes (2019). Estos últimos destacan que la prueba de Shapiro–Wilk permite evaluar si un conjunto de datos sigue una distribución normal. Sin embargo, cuando los datos presentan asimetría, no se cumplen los supuestos de normalidad, por lo que se recomienda aplicar transformaciones estadísticas o utilizar pruebas no paramétricas; dado que la muestra es de 160 expertos de una población conformada por estudiantes de los últimos ciclos de la carrera de Ingeniería de Software de la Universidad Nacional Mayor de San Marcos y especialistas en ciberseguridad de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú. Para la obtención de resultados, para lo cual se ha utilizado el software especializado en análisis estadístico SPSS.

Tabla 15
Prueba de normalidad

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Fraude informático	,344	160	,000	,636	160	,000
Seguridad de las transacciones y la protección de los datos	,363	160	,000	,634	160	,000
Ataques de Fake App	,350	160	,000	,636	160	,000
Ataques de SIM Swapping	,360	160	,000	,634	160	,000
Alta usabilidad y confiabilidad en la mitigación del fraude	,350	160	,000	,636	160	,000

Corrección de significación de Lilliefors

Teniendo en cuenta la prueba de normalidad de Kolmogorov Smirnov, se puede observar que tanto las variables como dimensiones presentan significancias menores al 0.05 por lo tanto se puede concluir que no presentan distribución normal, esto quiere decir que se debe usar una prueba no paramétrica, en este caso se usara la prueba ordinal el nivel de influencia entre las variables y sus dimensiones.

La prueba de Shapiro-Wilk aplicada a cada una de las variables y dimensiones del estudio arroja valores de significancia (Sig.) inferiores a 0.05, lo que indica que todas las distribuciones se desvían significativamente de una distribución normal. Esta prueba es especialmente recomendada para muestras menores a 200 observaciones, como es el caso ($n = 160$), debido a su mayor potencia estadística frente a otras pruebas de normalidad. Por lo tanto, estos resultados refuerzan la decisión de emplear pruebas no paramétricas en los análisis posteriores.

6.2.2. Hipótesis general

H_1 : El modelo Sectrabank mitiga significativamente los incidentes de fraude informático y es percibido positivamente en términos de accesibilidad, usabilidad y aceptación por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

H_0 : El modelo Sectrabank **no** mitiga significativamente los incidentes de fraude informático y **no** es percibido positivamente en términos de accesibilidad, usabilidad y aceptación por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Para evaluar esta relación, se aplicó la prueba de Chi-cuadrado siguiendo la metodología propuesta por Razikin y Soewito (2022), quienes estudiaron la correlación entre el diseño y desarrollo de medidas de ciberseguridad y su implementación en la mitigación de amenazas en sistemas de información. Asimismo, se consideraron factores como el uso de autenticación y el conocimiento de ataques cibernéticos, tal como lo señalan Shah y Agarwal (2020). Estos estudios respaldan la utilización del Chi-cuadrado como una herramienta estadística esencial para identificar patrones y determinar la

independencia entre variables en el contexto de la ciberseguridad. Asimismo, se aplicó la prueba de Chi-cuadrado, considerando la naturaleza categórica de las variables en estudio: tipo de fraude (SIM Swapping y Fake App), grupo de usuarios (experimental y control) y resultado de mitigación (fraude detectado y no detectado). Esta prueba permitió determinar si las diferencias observadas en la distribución de frecuencias entre los grupos resultaban estadísticamente significativas, garantizando que los hallazgos obtenidos no se deban al azar, sino al efecto real del modelo implementado

Investigaciones previas en el ámbito de la ciberseguridad han validado esta aproximación. Por ejemplo, Alrobaian et al. (2023) aplicaron el Chi-cuadrado en el análisis de la relación entre variables categóricas para evaluar la conciencia en ciberseguridad de los usuarios. Asimismo, Gupta y Kulariya (2016) emplearon el Chi-cuadrado como técnica de selección de atributos relevantes en un sistema de detección de intrusiones en grandes volúmenes de tráfico de red, evidenciando su utilidad en la mejora de precisión y eficiencia de los modelos de clasificación. En consecuencia, la aplicación del Chi-cuadrado en el modelo SectraBank no solo se justifica por la estructura de los datos experimentales, sino también por su pertinencia metodológica en investigaciones contemporáneas de ciberseguridad

Tabla 16
Prueba Chi cuadrado hipótesis general

	Valor	df	Significación asintótica (bilateral)	Significació n exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	140,647 ^a	1	,000		
Corrección de continuidad ^b	136,921	1	,000		
Razón de verosimilitud	177,490	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	139,768	1	,000		
N de casos válidos	160				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 39,50.

b. Sólo se ha calculado para una tabla 2x2

El análisis de la tabla 16 confirma la efectividad del modelo Sectrabank en la mitigación del fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android, mejorando la seguridad del usuario.

Específicamente, se observa en la fila "Chi-cuadrado de Pearson" y la columna "Significación asintótica (bilateral)" un valor de $p = 0.000$, indicando una relación estadísticamente significativa entre la implementación del modelo y la reducción del fraude. Asimismo, en la fila "Prueba exacta de Fisher" y las columnas "Significación exacta bilateral y unilateral" se registran también valores de $p = 0.000$, corroborando la existencia de dicha relación. Dado que el valor p es menor que el nivel de significación establecido (0.05), se rechaza la hipótesis nula y se acepta la hipótesis alternativa, lo que sugiere que el modelo Sectrabank tiene un impacto positivo en la mitigación de los incidentes de fraude informático y en términos de accesibilidad, usabilidad y aceptación por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

6.2.3. Hipótesis específica 1

H_1 : El modelo Sectrabank permite la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

H_0 : El modelo Sectrabank **no** permite la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Tabla 17
Prueba Chi cuadrado hipótesis específica 1

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	30,861 ^a	1	,000		
Corrección de continuidad ^b	29,123	1	,000		
Razón de verosimilitud	31,979	1	,000		
Prueba exacta de Fisher				,000	,000

Asociación lineal por lineal	30,668	1	,000		
N de casos válidos	160				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 33,50.

b. Sólo se ha calculado para una tabla 2x2

El análisis de la tabla 17 confirma que el modelo Sectrabank contribuye significativamente a mejorar la seguridad en las operaciones bancarias en Android, reduciendo la incidencia de fraude por Fake Apps y protegiendo los datos personales de los usuarios.

En particular, en la fila "Chi-cuadrado de Pearson" y la columna "Significación asintótica (bilateral)", se observa un valor de $p = 0.000$, asociado a un estadístico de $X^2 = 30.861$ con 1 grado de libertad ($df = 1$), indicando una relación estadísticamente significativa. Asimismo, en la fila "Prueba exacta de Fisher", tanto en la columna "Significación exacta bilateral" como en la columna "Significación exacta unilateral", se reporta también un valor de $p = 0.000$, indican una relación estadísticamente significativa entre el modelo Sectrabank y la mitigación del fraude en la modalidad de Fake App.

Dado que el valor p obtenido es menor que el nivel de significación establecido (0.05), se rechaza la hipótesis nula y se acepta la hipótesis alternativa, lo que respalda que el modelo Sectrabank permite la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

6.2.4. Hipótesis específica 2

H_1 : El modelo Sectrabank contribuye a la mitigación del fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

H_0 : El modelo Sectrabank **no** contribuye a la mitigación del fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Tabla 18
Prueba Chi cuadrado hipótesis específica 2

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	133,413 ^a	1	,000		
Corrección de continuidad ^b	129,783	1	,000		
Razón de verosimilitud	165,470	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	132,579	1	,000		
N de casos válidos	160				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 38,50.

b. Sólo se ha calculado para una tabla 2x2

El análisis de la tabla 18 respalda la efectividad del modelo Sectrabank en la mitigación de ataques de SIM Swapping en aplicaciones bancarias Android, reduciendo la tasa de éxito de estos fraudes y mejorando la seguridad de las transacciones electrónicas.

De acuerdo con los resultados, en la fila "Chi-cuadrado de Pearson" y la columna "Significación asintótica (bilateral)", se obtuvo un valor de $p = 0.000$, asociado a un estadístico de $X^2 = 133.413$ con 1 grado de libertad ($df = 1$), evidenciando una asociación estadísticamente significativa. Asimismo, en la fila "Prueba exacta de Fisher", tanto en la columna "Significación exacta bilateral" como en la columna "Significación exacta unilateral", se registraron valores de $p = 0.000$, indican una asociación estadísticamente significativa entre el modelo Sectrabank y la reducción del fraude por SIM Swapping.

Dado que el valor p obtenido es menor que el nivel de significación establecido (0.05), se rechaza la hipótesis nula y se acepta la hipótesis alternativa, confirmando que el modelo Sectrabank contribuye a la mitigación del fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android

6.2.5. Hipótesis específica 3

H₁: El modelo Sectrabank es percibido como accesible, comprensible y fácil de usar por los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

H₀: El modelo Sectrabank **no** es percibido como accesible, comprensible y fácil de usar por los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Tabla 19
Prueba Chi cuadrado hipótesis específica 3

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	116,254 ^a	1	,000		
Corrección de continuidad ^b	112,860	1	,000		
Razón de verosimilitud	139,046	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	115,527	1	,000		
N de casos válidos	160				

El análisis de la tabla 19 demuestra que el modelo Sectrabank tiene una percepción positiva por los usuarios en términos de accesibilidad, comprensión y facilidad de uso en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Los resultados obtenidos en la fila "Chi-cuadrado de Pearson" y la columna "Significación asintótica (bilateral)", se obtuvo un valor de $p = 0.000$, asociado a un estadístico de $X^2 = 116.254$ con 1 grado de libertad ($df = 1$), indicando una asociación significativa entre la implementación del modelo y la reducción del fraude. De igual forma, en la fila "Prueba exacta de Fisher", tanto en la columna "Significación exacta bilateral" como en la columna "Significación exacta unilateral", se reporta un valor de $p = 0.000$, indican que existe una relación estadísticamente significativa entre el modelo Sectrabank y la percepción positiva de usabilidad por parte de los usuarios lo que

confirma que el modelo Sectrabank es percibido como accesible, comprensible y fácil de usar por los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android

6.2.6. Hipótesis específica 4

H₁: El modelo Sectrabank es aceptado por los usuarios como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

H₀: El modelo Sectrabank **no** es aceptado por los usuarios como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Tabla 20
Prueba Chi cuadrado hipótesis específica 4

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	140,823 ^a	1	,000		
Corrección de continuidad ^b	137,093	1	,000		
Razón de verosimilitud	179,068	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	139,943	1	,000		
N de casos válidos	160				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 38,50.

b. Sólo se ha calculado para una tabla 2x2

El análisis de la tabla 20 confirma que los usuarios están dispuestos a adoptar Sectrabank como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Los resultados obtenidos que se muestra en la fila "Chi-cuadrado de Pearson" y la columna "Significación asintótica (bilateral)", se registró un valor de $p = 0.000$,

correspondiente a un estadístico de $X^2 = 140.823$ con 1 grado de libertad ($df = 1$), lo que demuestra una asociación estadísticamente significativa. Igualmente, en la fila "Prueba exacta de Fisher", en las columnas de "Significación exacta bilateral" y "Significación exacta unilateral", se observó un valor de $p = 0.000$, indican que existe una relación estadísticamente significativa entre el modelo Sectrabank y la percepción de confianza por parte de los usuarios.

Dado que el valor p obtenido es menor que el nivel de significación establecido (0.05), se rechaza la hipótesis nula y se acepta la hipótesis alternativa, confirmando que los usuarios validan el modelo Sectrabank como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

6.3. Análisis e interpretación de la información

En la presente sección, se lleva a cabo un análisis crítico y comprehensivo de los datos generados durante el trabajo de campo, con la finalidad de interpretar los hallazgos en función de los objetivos e hipótesis establecidas. Esta interpretación es apoyada no solo por el marco teórico supuesto sino también por varios estudios existentes en el campo de ciberseguridad y seguridad de la información.

El modelo Sectrabank fue validado mediante un diseño cuasi-experimental para 160 usuarios, conformado por un grupo experimental de 80 usuarios que utilizaron el modelo con la implementación de las medidas de seguridad y a un grupo de control de 80 usuarios que utilizaron el modelo Sectrabank, sin las medidas de seguridad. A lo largo del experimento, se recolectaron datos tanto cuantitativos como cualitativos utilizando instrumentos previamente validados, incluyendo cuestionarios estructurados y pruebas funcionales.

Para el análisis estadístico, se empleó el software SPSS, permitiendo identificar patrones de vulnerabilidad, evaluar el impacto de las medidas de seguridad implementadas y analizar la eficacia en la reducción del éxito de los ataques. Adicionalmente, se incorporó una interpretación cualitativa basada en la experiencia declarada por los usuarios, cuyos testimonios se sistematizaron en el Anexo 5, titulado:

Informe del grupo control y experimental con respecto a la usabilidad percibida por los usuarios.

Es importante destacar que, luego de realizar el trabajo de campo en un entorno controlado tanto para el grupo experimental como para el grupo de control, se determinó que el modelo Sectrabank mitiga significativamente los ataques de fraude informático en las modalidades de Fake App y SIM Swapping, con una eficacia del 97,50 % en la mitigación de ataques de Fake App y del 76,25 % frente a SIM Swapping. Asimismo, el modelo fue validado por los usuarios como fácil de usar en un 96,25 % y confiable en un 95 %. Estos resultados respaldan y sustentan la hipótesis general que plantea que: “El modelo Sectrabank mitiga significativamente los incidentes de fraude informático y es percibido positivamente en términos de accesibilidad, usabilidad y aceptación por parte de los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.”

Estos hallazgos se alinean con las recomendaciones de (Bassolé et al., 2020) y (Ukpe et al., 2022), quienes resaltan la importancia de implementar soluciones de seguridad digital que no interfieran negativamente con la experiencia del usuario. Además, el diseño multicapa del modelo Sectrabank que integra autenticación biométrica, validación del IMEI y geolocalización se fundamenta en los principios de la teoría de la seguridad de la información (Whitman y Mattord, 2017) y la teoría de la ingeniería social (Mitnick y Vamosi, 2002), lo que permite bloquear vectores comunes de suplantación de identidad y captura de códigos OTP.

A fin de facilitar la interpretación sistemática de los hallazgos experimentales para las hipótesis específicas, el presente análisis se divide en cuatro subdimensiones, conforme se describe a continuación:

a) Mitigación del fraude por Fake App

Durante la simulación de ataques en la modalidad Fake App, realizada en un entorno controlado, el grupo experimental logró bloquear 78 de los 80 intentos, alcanzando una eficacia del 97,50 %. En contraste, en el grupo de control, 75 de los 80 participantes fueron vulnerados, lo que representa un 93,75 % de ataques exitosos. Estos

resultados evidencian que el modelo Sectrabank permite la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

b) Mitigación del fraude por SIM Swapping

En el contexto de evaluación de vulnerabilidad ante ataques de SIM Swapping, el grupo experimental logró mitigar 61 de 80 intentos de fraude, lo que representa una efectividad del 76,25 %. En contraste, en el grupo de control, 54 de los 80 dispositivos fueron vulnerados, alcanzando un 67,50 % de ataques exitosos. Estos hallazgos ponen en evidencia que el modelo Sectrabank contribuye a la mitigación del fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

c) Percepción de accesibilidad, comprensión y facilidad de uso

Luego de realizar las pruebas controladas frente a ataques de fraude informático en las modalidades de Fake App y SIM Swapping, se evaluó la percepción de usabilidad del modelo Sectrabank. El grupo experimental, conformado por 80 usuarios que contaban con las medidas de seguridad implementadas, y el grupo de control, también integrado por 80 participantes, pero sin acceso a dichas medidas, brindaron información relevante. En el grupo experimental, 77 de los 80 usuarios que representa el 96,25 % evaluaron positivamente la usabilidad del modelo, considerándolo comprensible y fácil de usar. Es destacable que, incluso en el grupo de control, 9 de los 80 usuarios que representa el 11,25 % también percibieron el modelo como usable, a pesar de no contar con los mecanismos de seguridad activados, evidenciándose que el modelo Sectrabank es aceptado por los usuarios como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Estos resultados se alinean con los principios de experiencia del usuario planteados por Sauro y Lewis (2016), quienes sostienen que la percepción de accesibilidad, comprensión y facilidad de uso son factores clave para la aceptación de tecnologías en contextos móviles y de alta seguridad.

d) Aceptación del modelo: confiabilidad, eficacia y adaptabilidad

Los usuarios del grupo experimental que fueron expuestos a ataques de fraude informático en las modalidades de Fake App y SIM Swapping manifestaron una alta percepción de confiabilidad respecto al modelo Sectrabank. En específico, 76 de los 80 encuestados que representa el 95 %, consideraron que el modelo es confiable para realizar operaciones electrónicas a través de dispositivos móviles. Estos hallazgos ponen en evidencia que el modelo Sectrabank es aceptado por los usuarios como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android

6.4. Análisis de resultados estadísticos

A partir de los resultados obtenidos tras la aplicación de las pruebas estadísticas, se observa que el modelo Sectrabank constituye una alternativa efectiva para la mitigación del fraude informático en operaciones electrónicas bancarias en dispositivos móviles Android. En la fila "Chi-cuadrado de Pearson" y la columna "Significación asintótica (bilateral)", se registraron valores de $p = 0.000$, asociados a estadísticos chi-cuadrado de 140,647 (Tabla 16), 30,861 (Tabla 17), 133,413 (Tabla 18), 116,254 (Tabla 19) y 140,823 (Tabla 20), respectivamente, todos con 1 grado de libertad.

Complementariamente, en la fila "Prueba exacta de Fisher", tanto en la columna "Significación exacta bilateral" como en la "Significación exacta unilateral", se observaron también valores de $p = 0.000$ en todas las tablas, lo que reafirma los hallazgos obtenidos. Dado que los valores de p obtenidos son inferiores al nivel de significancia establecido (0.05), se rechaza en todos los casos la hipótesis nula y se acepta la hipótesis alternativa, evidenciando una relación estadísticamente significativa entre la implementación del modelo Sectrabank y la reducción del fraude informático en aplicaciones bancarias Android.

Asimismo, se destaca que no se presentaron casillas con recuentos esperados menores a 5 en ninguna de las tablas analizadas, cumpliéndose de esta manera los supuestos necesarios para la validez de la prueba de chi-cuadrado. En conjunto, los resultados confirman que la aplicación del modelo Sectrabank mejora de manera

significativa la seguridad en transacciones electrónicas, contribuyendo de forma efectiva a la mitigación del fraude informático en las modalidades de Fake App y Sim Swapping.

6.5. Discusión de resultados

El análisis del estado del arte revela que la mayoría de los estudios sobre fraude en aplicaciones bancarias móviles han seguido una metodología centrada en la aplicación de modelos de Machine Learning y Deep Learning sobre datasets controlados. Por ejemplo, Wang et al. (2018) utilizaron Random Forest alcanzando hasta 99 % de precisión, Gezer et al. (2019) emplearon TLSH + MinHash con porcentajes elevado, y Udayakumar et al. (2024) implementaron GIST con FFNN logrando hasta un 98 %. Si bien estos resultados son elevados, su principal limitación radica en que los modelos se evaluaron en condiciones de laboratorio, sin validar su aplicabilidad en entornos reales con usuarios finales.

En contraste, el modelo SectraBank adoptó una metodología cuasi-experimental, con un diseño que incluyó un grupo de control y grupo experimental, lo que permitió evaluar la eficacia del modelo en condiciones prácticas. Bajo esta metodología, SectraBank demostró ser altamente eficaz frente al fraude por Fake App, al identificar y bloquear el 97,5 % de los intentos de fraude. Este resultado no solo valida la precisión del modelo, sino que confirma su validez externa al haberse probado con usuarios reales y no únicamente en entornos simulados, conforme lo planten los modelos implementados por Gezer et al. (2019) y Udayakumar et al. (2024).

En relación con el SIM Swapping, los trabajos de Kim et al. (2022) y Oh et al. (2023) presentaron enfoques innovadores basados en autenticación multifactor con tokens físicos, blockchain y biometría, así como la detección de SIM Box mediante huellas digitales. Aunque teóricamente robustos, dichos modelos presentan limitaciones metodológicas: dependencia de datasets reducidos, altos costos de infraestructura y riesgo de falsos positivos. Frente a ello, Sectrabank logró mitigar el 76,25 % de los intentos de fraude por SIM Swapping, combinando de manera inédita el uso de IMEI único, autenticación biométrica y geomalla de geolocalización en tiempo real, no

dependiendo de datos históricos como los estudios realizados por Kim et al. (2022) y Oh et al. (2023).

En cuanto a la experiencia del usuario, la literatura disponible se ha concentrado principalmente en métricas técnicas, sin valorar de manera sistemática la aceptación o facilidad de uso de los sistemas de seguridad. Trabajos como los de Awad et al. (2024), Khan et al. (2023) y Ali et al. (2021) demostraron la eficacia de sistemas multimodales y de autenticación con OTP y blockchain, pero omitieron la evaluación de percepción y usabilidad. SectraBank, en cambio, integró criterios de accesibilidad, comprensión y facilidad de uso, logrando una aceptación del 96,25 % de los usuarios, quienes percibieron la aplicación como intuitiva y amigable y la confianza del 95% de los usuarios. Estos resultados no solo demuestran la eficacia técnica, sino también el alineamiento con las expectativas de los usuarios, un factor clave para la adopción real de cualquier solución de seguridad bancaria.

En síntesis, mientras que los modelos revisados se enfocan en componentes aislados ya sea algoritmos de clasificación, autenticación multifactor o biometría, el modelo Sectrabank integra de manera armónica tres pilares de seguridad (IMEI único, biometría y geolocalización) dentro de una misma arquitectura, validada experimental y estadísticamente. Su metodología combinó pruebas de hipótesis, métricas de rendimiento y evaluación de usabilidad, consolidándole, así como una propuesta robusta, práctica y escalable frente al creciente desafío del fraude informático en las modalidades de Fake App y SIM Swapping.

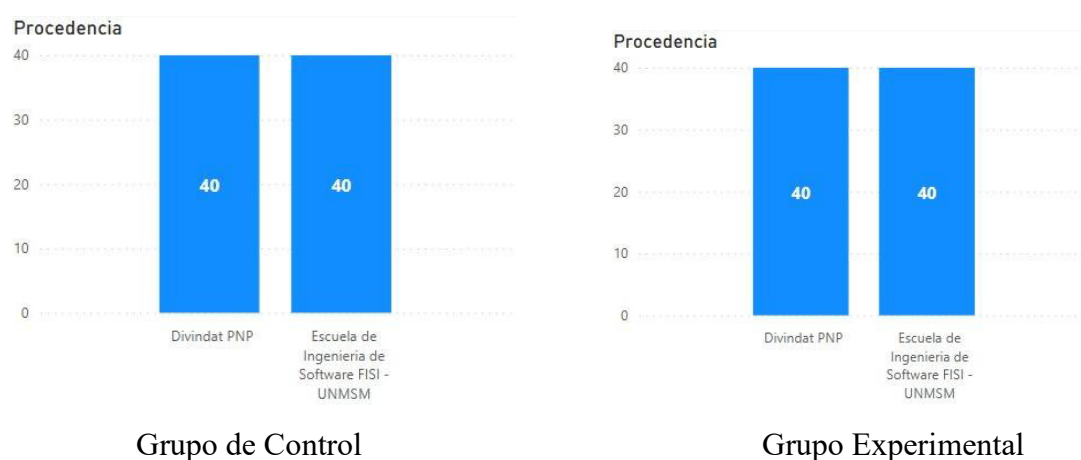
6.6. Presentación de resultados

La distribución de los usuarios que participaron en la evaluación de la aplicación se presenta en la Figura 20. Se conformaron dos grupos: un grupo de control, integrado por 80 usuarios, de los cuales 40 correspondieron a estudiantes de la Escuela Profesional de Ingeniería de Software de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos (UNMSM) y 40 a especialistas de la

División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú.

De manera análoga, se estructuró el grupo experimental con 80 usuarios, siguiendo la misma proporción entre estudiantes y especialistas. En total, la muestra estuvo constituida por 160 participantes, distribuidos equitativamente entre los dos grupos de estudio.

Figura 20
Representación de la población

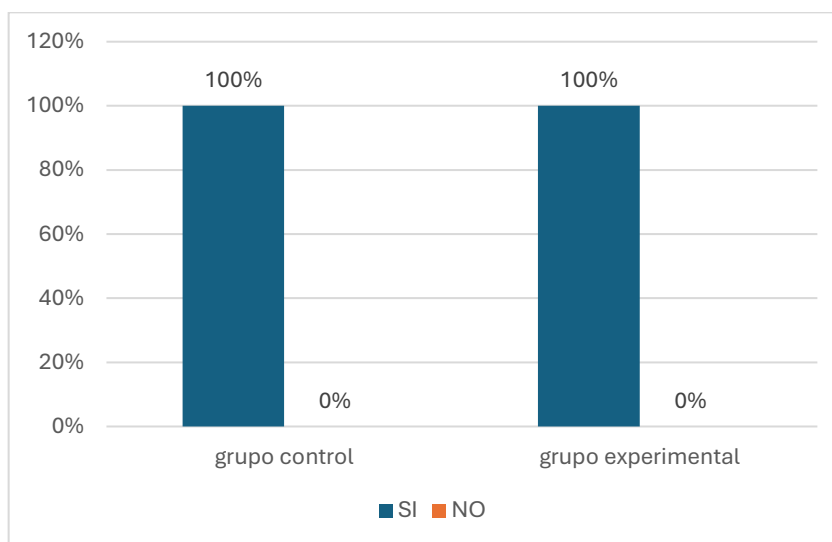


En la tabla 21 y figura 21 muestran que el 100% de los encuestados en ambos grupos (control y experimental) realizan operaciones bancarias, lo que indica que todos los participantes tienen experiencia en el uso de servicios financieros digitales. La gráfica confirma visualmente esta uniformidad, con barras del mismo tamaño para ambos grupos en la categoría "Sí".

Tabla 21
Operaciones bancarias

	Grupo control		Grupo experimental	
	f	%	f	%
si	80	100%	80	100%
no	0	0%	0	0%
total	80	100%	80	100%

Figura 21
Gráfica de Operaciones bancarias



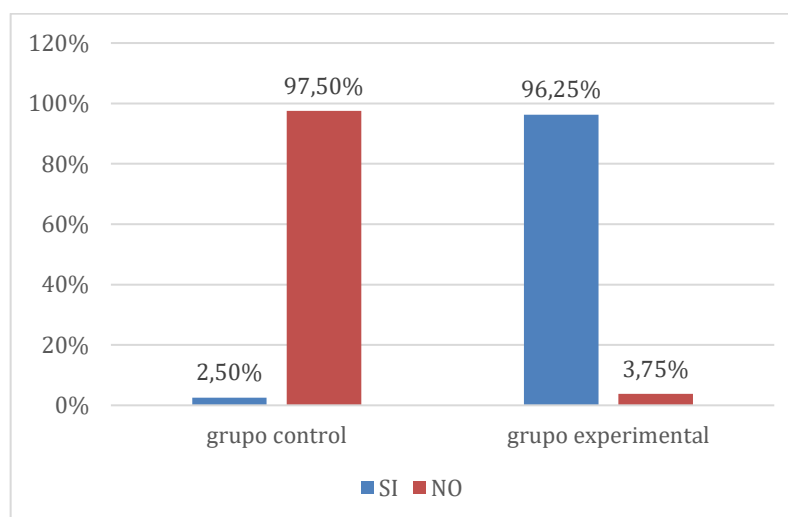
En la tabla 22 y figura 22, en el grupo control el 97.50% de los encuestados indica que el modelo Sectrabank no ayuda a mitigar el fraude informático en operaciones; sin embargo, en el grupo experimental el 96.25% respondió que, si ayudo a mitigar, lo que sugiere una alta mitigación sobre los riesgos de seguridad informática. La gráfica refuerza estos resultados, mostrando que todos los participantes respondieron afirmativamente.

Tabla 22
Frecuencia de respuestas sobre la efectividad del modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias.

	Grupo control		Grupo experimental	
	f	%	f	%
si	2	2,50%	77	96,25%
no	78	97,50%	3	3,75%
total	80	100%	80	100%

Tabla 23

Gráfica sobre la percepción de mitigación del fraude informático en operaciones electrónicas mediante el modelo Sectrabank

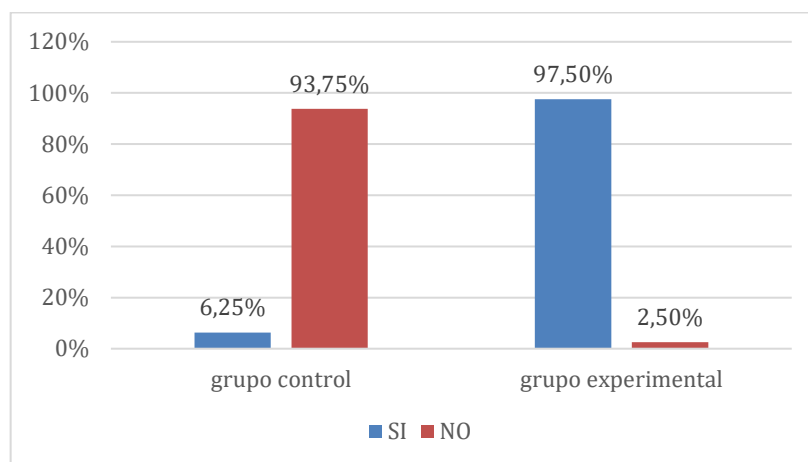


En la tabla 23 y figura 23 se observa que el 93,75% de los encuestados del grupo de control indican que el modelo no mitigó el fraude informático en la modalidad Fake App, por otro lado, en el grupo experimental el 97,50% respondió que, si mitigó el ataque, lo que demuestra que el modelo Sectrabank permite la detección eficaz del fraude informático en la modalidad de Fake App en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Tabla 24

Frecuencia de respuestas sobre la efectividad del modelo Sectrabank para mitigar el fraude informático en la modalidad de Fake App

	Grupo control		Grupo experimental	
	f	%	f	%
si	5	6,25%	78	97,50%
no	75	93,75%	2	2,50%
total	80	100%	80	100%

Figura 22**Gráfica sobre la percepción de mitigación del fraude informático por Fake App**

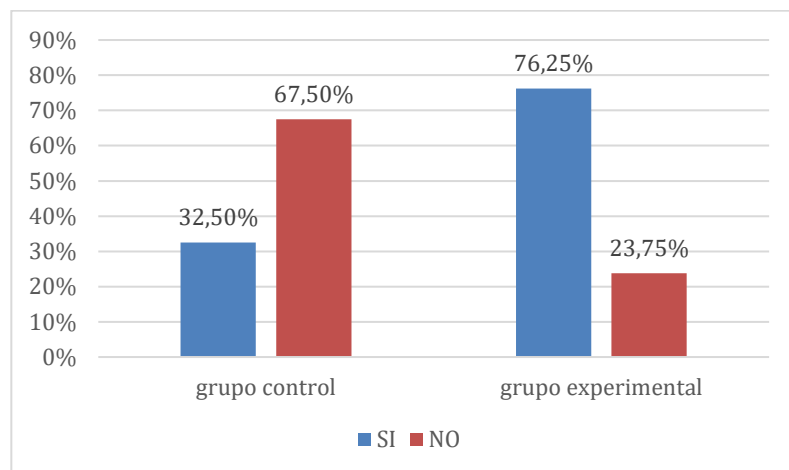
En la tabla 24 y figura 24 se observa que el 67.50% de los encuestados del grupo de control indican que el modelo no mitigo el fraude informático en la modalidad SIM Swapping, por otro lado, en el grupo experimental el 76,25% respondió que, si mitigó el ataque. Dado que estos resultados son coherentes con el análisis estadístico de la prueba de chi-cuadrado, se valida la hipótesis específica 2, confirmando que: El modelo Sectrabank contribuye a la mitigación del fraude informático en la modalidad de SIM Swapping en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android.

Tabla 25**Frecuencia de respuestas sobre la efectividad del modelo Sectrabank para mitigar el fraude informático en la modalidad de SIM Swapping**

	Grupo control		Grupo experimental	
	f	%	f	%
si	26	32,50%	61	76,25%
no	54	67,50%	19	23,75%
total	80	100%	80	100%

Figura 23

Gráfica sobre la percepción de mitigación del fraude informático mediante SIM Swapping



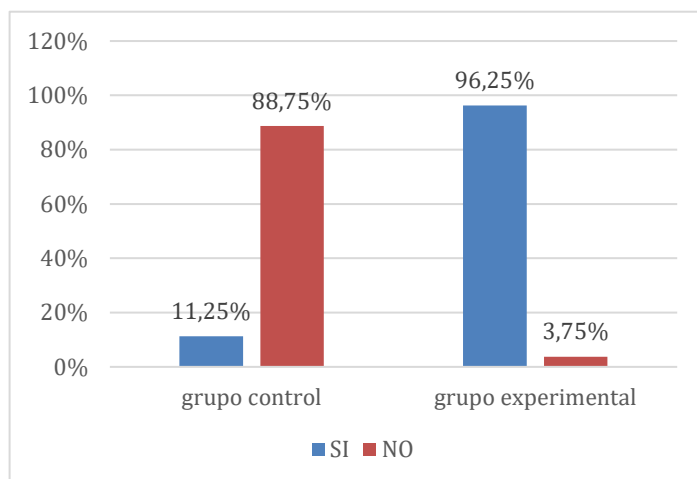
En la tabla 25 y figura 25 se observa que el solo el 11,25% del grupo de control no perciben al modelo Sectrabank como una aplicación amigable y fácil de utilizar, sin embargo el 96,25% del grupo experimental si lo perciben como una aplicación de alta usabilidad, Dado que estos resultados son coherentes con el análisis estadístico de la prueba de chi-cuadrado, se valida la hipótesis específica 3, confirmando que: El modelo Sectrabank es percibido como accesible, comprensible y fácil de usar por los usuarios en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android

Tabla 26

Percepción de usabilidad del modelo Sectrabank

	grupo control		grupo experimental	
	f	%	f	%
si	9	11,25%	77	96,25%
no	71	88,75%	3	3,75%
total	80	100%	80	100%

Figura 24
Gráfica de Percepción de usabilidad del modelo Sectrabank



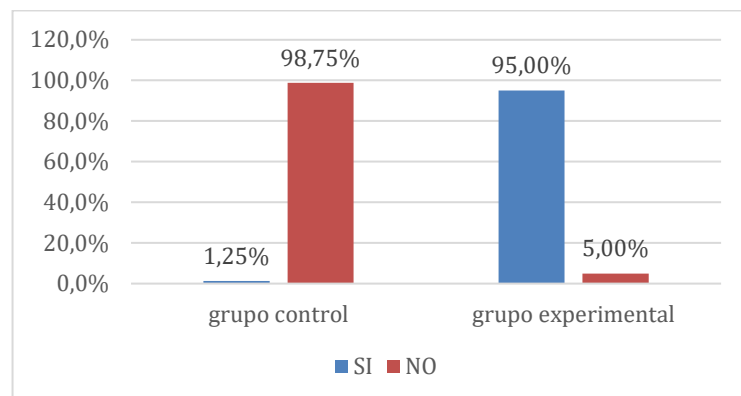
En la tabla 26 y figura 26 se observa que el 95% del grupo experimental está dispuesto a utilizar la aplicación propuesta, en contraste con solo el 1,25% del grupo control. La gráfica representa esta disparidad, con una mayoría del grupo experimental mostrando interés en el uso de la aplicación, esto sugiere que la propuesta es bien recibida por quienes la han probado y percibido su efectividad. Dado que estos resultados son coherentes con el análisis estadístico de la prueba de chi-cuadrado, se valida la hipótesis específica 4, confirmando que: El modelo Sectrabank es aceptado por los usuarios como una solución confiable, eficaz y adaptable para la prevención del fraude informático en operaciones electrónicas realizadas a través de aplicaciones bancarias en dispositivos Android

Tabla 27
Frecuencia respecto a la percepción de la confiabilidad del modelo Sectrabank

	grupo control		grupo experimental	
	f	%	f	%
si	1	1,25%	76	95,00%
no	79	98,75%	4	5,00%
total	80	100%	80	100%

Figura 25

Gráfica respecto a la percepción de la confiabilidad del modelo Sectrabank



CAPÍTULO 7: CONCLUSIONES Y RECOMENDACIONES.

7.1. Conclusiones

La creación e implementación del modelo Sectrabank, junto con las pruebas controladas realizadas a una muestra de 160 participantes, distribuidos en un grupo experimental y otro de control, demostraron que este enfoque es capaz de reducir de manera efectiva el fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android. Los resultados mostraron una disminución notable de incidentes, especialmente en los casos de Fake App y SIM Swapping. Además, los usuarios, consideraron a Sectrabank como una herramienta segura, confiable y sencilla de utilizar, cumpliendo así con los criterios de eficacia, accesibilidad y usabilidad planteados en el objetivo general.

El modelo Sectrabank demostró ser altamente eficaz en la detección del fraude informático asociado a la modalidad de Fake App, al lograr identificar y bloquear el 97,5 % de los intentos de fraude durante las pruebas controladas. Este hallazgo confirma que el modelo cumple con el objetivo de reforzar la seguridad frente a aplicaciones fraudulentas, cuya validez fue respaldada estadísticamente mediante la prueba de hipótesis específica, con un nivel de significación de $p = 0.000$, valor claramente inferior al umbral convencional de 0.05.

La incorporación de mecanismos funcionales y tecnológicos en el modelo Sectrabank permitió mitigar el 76,25 % de los intentos de fraude por SIM Swapping en operaciones electrónicas realizadas mediante aplicaciones bancarias en dispositivos Android. Este resultado evidencia un fortalecimiento de la autenticación y de la seguridad en las transacciones, lo que contribuye directamente a la protección del usuario. La eficacia en la mitigación fue comprobada de manera experimental y se encuentra respaldada estadísticamente por la prueba de hipótesis, con un nivel de significancia de $p = 0.000$, valor claramente inferior al umbral convencional de 0.05.

El modelo Sectrabank incorporó características de accesibilidad, claridad y facilidad de uso que fueron valoradas de manera positiva por el 96,25 % de los usuarios. La mayoría lo percibió como una aplicación intuitiva y amigable para realizar operaciones

bancarias en dispositivos Android, resaltando además que su funcionamiento resultó fácil de comprender y utilizar. Estos hallazgos confirman que Sectrabank logró integrar componentes centrados en el usuario, lo que facilitó la adopción de medidas de seguridad sin provocar frustración ni dificultades innecesarias.

Los criterios de confiabilidad, eficacia y adaptabilidad aplicados en el desarrollo del modelo Sectrabank alcanzaron una aceptación del 95 % entre los usuarios que participaron en las simulaciones de operaciones electrónicas en dispositivos Android dentro de un entorno controlado. Los participantes lo calificaron como una herramienta segura y efectiva, mostrando además una alta disposición para emplearla en la protección de sus transacciones bancarias. Esta valoración confirma que el modelo cumple con los estándares de confianza y adaptabilidad, consolidando a Sectrabank como una solución sólida y acorde a las expectativas de seguridad de los usuarios. Dichos resultados fueron validados estadísticamente mediante la prueba de hipótesis.

7.2. Recomendaciones

Se recomienda implementar Sectrabank en entornos reales de la banca móvil, aprovechando la eficacia comprobada para proteger a los clientes frente a fraudes informáticos en las modalidades de Fake App y SIM Swapping. Del mismo modo, resulta conveniente realizar actualizaciones periódicas que permitan adaptarlo a las nuevas técnicas de ataque, así como involucrar activamente a los usuarios mediante procesos de educación y soporte. De esta forma, se fortalecerán la confianza, la seguridad y la usabilidad de la solución a lo largo del tiempo.

Se recomienda integrar las funcionalidades de detección de Fake Apps de Sectrabank dentro de las aplicaciones bancarias ya existentes y en los procesos de publicación de nuevas aplicaciones móviles. Asimismo, resulta fundamental mantener actualizadas las bases de datos de aplicaciones maliciosas y optimizar de manera continua los algoritmos de detección, con el fin de anticipar y neutralizar las nuevas variantes de fraude. Finalmente, la educación de los usuarios para que descarguen únicamente aplicaciones desde fuentes oficiales reforzará la eficacia del modelo y contribuirá a minimizar el riesgo de instalación de aplicaciones bancarias falsas.

Se recomienda incorporar mecanismos complementarios al modelo Sectrabank, como la implementación de alertas en tiempo real ante cambios de SIM CARD, con el propósito de reforzar la protección frente a ataques de SIM Swapping. Del mismo modo, resulta conveniente establecer alianzas estratégicas con los operadores móviles, que permitan detectar y responder de manera temprana a posibles intentos de duplicación de tarjetas SIM. Finalmente, mantener una vigilancia constante y actualizar el modelo frente a las nuevas técnicas utilizadas en este tipo de fraude garantizará que Sectrabank se mantenga como una solución eficaz y adaptable en la mitigación de estas amenazas.

Se recomienda mantener al usuario como eje central en el desarrollo continuo de Sectrabank, procurando que las futuras mejoras o nuevas funciones conserven su simplicidad y claridad de uso. Asimismo, es fundamental recoger e incorporar de manera periódica la retroalimentación de los usuarios, con el fin de perfeccionar la experiencia de uso y asegurar que las medidas de seguridad resulten comprensibles y accesibles para personas con distintos niveles de conocimiento técnico.

Se recomienda impulsar la adopción del modelo Sectrabank tanto entre los usuarios como en las instituciones bancarias, resaltando su confiabilidad y eficacia comprobada en la prevención del fraude. Para mantener esta confianza en el tiempo, resulta esencial actualizar periódicamente sus mecanismos frente a nuevas amenazas y asegurar su adaptabilidad a distintos entornos y dispositivos. Asimismo, la implementación de programas piloto y campañas informativas permitirá evaluar su desempeño en contextos reales y fortalecer su imagen como una solución robusta de ciberseguridad bancaria. Finalmente, se propone uniformizar las medidas de seguridad en todas las aplicaciones bancarias del país, extendiendo su aplicación también a dispositivos con sistemas iOS y a nuevas tecnologías que ingresen al mercado, con el fin de establecer un estándar común que refuerce la protección de las operaciones electrónicas.

Como línea de trabajo futuro, se recomienda ampliar el alcance del modelo Sectrabank hacia la mitigación de fraudes informáticos en operaciones realizadas desde computadoras personales, dado que los entornos de escritorio continúan siendo un objetivo atractivo para los ciberdelincuentes. Asimismo, resulta necesario explorar mecanismos de defensa frente a ataques apoyados en tecnologías emergentes, como la

computación cuántica, cuyo poder de procesamiento podría representar una amenaza para los sistemas criptográficos tradicionales. Del mismo modo, se plantea investigar estrategias que contrarresten técnicas de ataque basadas en inteligencia artificial, considerando que estas herramientas facilitan la creación de patrones de fraude más sofisticados y difíciles de detectar.

REFERENCIAS BIBLIOGRÁFICAS

- Abi Din, Z., Venugopalan, H., Lin, H., Wushensky, A., Liu, S., & King, S. T. (2021, May). *Doing good by fighting fraud: Ethical anti-fraud systems for mobile payments*. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 1623–1640). IEEE. <https://doi.org/10.1109/SP40001.2021.00110>
- Akande, O., Gbenle, O., Abikoye, O., Jimoh, R., Akande, H., Balogun, A. y Fatokun, A. (2023). SMSPROTECT: An automatic smishing detection mobile application. *ICT Express*, 9(2), 168-176. doi:<https://doi.org/10.1016/j.icte.2022.05.009>
- Alani, M. y Tawfik, H. (2022). Phishnot: A cloud-based machine-learning approach to phishing url detection. *Computer Networks*, 218, 109407. doi:<https://doi.org/10.1016/j.comnet.2022.109407>
- Alatawi, M. N. (2025). Detection of fraud in IoT based credit card collected dataset using machine learning. *Machine Learning with Applications*, 19, 100603. DOI: <https://doi.org/10.1016/j.mlwa.2024.100603>
- Alabdulatif, A., Samarasinghe, R., & Thilakarathne, N. N. (2023). *A novel robust geolocation-based multi-factor authentication method for securing ATM payment transactions*. *Applied Sciences*, 13(19), 10743. <https://doi.org/10.3390/app131910743>
- Ali, G., Dida, M. A., & Elikana Sam, A. (2021). *A secure and efficient multi-factor authentication algorithm for mobile money applications*. *Future Internet*, 13(12), 299. <https://doi.org/10.3390/fi13120299>
- Aljofey, A., Jiang, Q., Qu, Q., Huang, M. y Niyigena, J. (2020). An effective phishing detection model based on character level convolutional neural network from URL. *Electronics*, 9(9), 1514. doi:<https://doi.org/10.3390/electronics9091514>

- Alsunaidi, S. J., & Almuhaideb, A. M. (2021). *A strong smartphone authentication model to control cellular network access using blockchain*. *Wireless Networks*, 27(4), 2301–2321. <https://doi.org/10.1007/s11276-021-02542-0>
- Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). *Cybersecurity awareness assessment among trainees of the Technical and Vocational Training Corporation*. **Big Data and Cognitive Computing**, 7(2), 73. <https://doi.org/10.3390/bdcc7020073>
- Almseidin, M., Alkasassbeh, M., Alzubi, M. y Al-Sawwa, J. (2022). Cyber-phishing website detection using fuzzy rule interpolation. *Cryptography*, 6(2), 24. doi:<https://doi.org/10.3390/cryptography6020024>
- Almuhaideb, A., Aslam, N., Alabdullatif, A., Altamimi, S., Alothman, S., Alhussain, A. y Alissa, K. (2022). Homoglyph attack detection model using machine learning and hash function. *Journal of Sensor and Actuator Networks*, 11(3), 54. doi:<https://doi.org/10.3390/jsan11030054>
- Alqahtani, H., Alotaibi, S., Alrayes, F., Al-Turaiki, I., Alissa, K., Aziz, A. y Al Duhayyim, M. (2022). Evolutionary algorithm with deep auto encoder network based website phishing detection and classification. *Applied Sciences*, 12(15), 7441.
- Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q., Saleem, K. y Faheem, M. (2023). A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. *Electronics*, 12(1), 232. doi:<https://doi.org/10.3390/electronics12010232>.
- Althobaiti, K., Vaniea, K., Wolters, M. y Alsufyani, N. (2023). Using Clustering Algorithms to Automatically Identify Phishing Campaigns. *IEEE Access*. doi:<https://doi.org/10.1109/ACCESS.2023.3310810>
- Alvarado, C., Pingo, C., y Mendoza, A. (2022). Revisión de la implementación del machine learning en la seguridad de la información. *Campus*, 27(34), 365-378. <https://doi.org/10.24265/campus.2022.v27n34.13>

- Alzomai, M. H. (2011). *Identity management: Strengthening one-time password authentication through usability* (Doctoral dissertation, Queensland University of Technology).
- Anjum, M., Iqbal, S. y Hamelin, B. (2022). ANUBIS: a provenance graph-based framework for advanced persistent threat detection. n Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, 1684-1693. doi:<https://doi.org/10.1145/3477314.3507097>
- Armstrong, M., Jones, K. y Namin, A. (2023). How Perceptions of Caller Honesty Vary During Vishing Attacks That Include Highly Sensitive or Seemingly Innocuous Requests. *Human Factors*, 65(2), 275-287. doi:10.1177/00187208211012818
- Arslan, R. (2021). AndroAnalyzer: android malicious software detection based on deep learning. *PeerJ Computer Science*, 7. doi:<https://doi.org/10.7717/peerj-cs.533>
- Arunakumari, B., Shrivathsa, P. y Vinodkumar, G. (2022). Attack and Defense Methodology Against the Share Intents in Android. *Sustainable Technology and Advanced Computing in Electrical Engineering: Proceedings of ICSTACE 2021*, 141-152. doi:https://doi.org/10.1007/978-981-19-4364-5_12
- Asiri, S., Xiao, Y. y Li, T. (2023). PhishTransformer: A Novel Approach to Detect Phishing Attacks Using URL Collection and Transformer. *Electronics*, 13(1), 30. doi:<https://doi.org/10.3390/electronics13010030>
- Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). *AI-powered biometrics for Internet of Things security: A review and future vision*. *Journal of Information Security and Applications*, 82, 103748. <https://doi.org/10.1016/j.jisa.2024.103748>
- Baena Paz, G. (2017). *Metodología de la investigación*. Grupo Editorial Patria.

- Bairwa, A. K., & Joshi, S. (2021). *Mutual authentication of nodes using session token with fingerprint and MAC address validation*. Egyptian Informatics Journal, 22(4), 479–491. <https://doi.org/10.1016/j.eij.2021.03.003>
- Babbie, E. R. (2010). *The practice of social research* (12.^a ed.). Wadsworth Cengage Learning.
- Bassolé, D., Koala, G., Traoré, Y., & Sié, O. (2020). Vulnerability analysis in mobile banking and payment applications on android in African Countries. In *Innovations and Interdisciplinary Solutions for Underserved Areas: 4th EAI International Conference, InterSol 2020, Nairobi, Kenya, March 8-9, 2020, Proceedings 4* (pp. 164-175). Springer International Publishing.
- Bartłomiejczyk, M., El Fray, I., Kurkowski, M., Szymoniak, S., & Siedlecka-Lamch, O. (2022). *User Authentication Protocol Based on the Location Factor for a Mobile Environment*. IEEE Access, 10, 16439–16453. <https://doi.org/10.1109/ACCESS.2022.314853>
- Bedari, A., Wang, S., & Yang, W. (2022). *A secure online fingerprint authentication system for industrial IoT devices over 5G networks*. Sensors, 22(19), 7609. <https://doi.org/10.3390/s22197609>
- Bello, N. o. A., & Olufemi, N. K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505-1520. <https://doi.org/10.51594/csitrj.v5i6.1252>
- Berbecaru, D. G. (2025). *SAM-PAY: A location-based authentication method for mobile environments*. Electronics, 14(3), 621. <https://doi.org/10.3390/electronics1403062>
- Brown, D., Batra, G., Zafar, H., & Saeed, K. (2024). Reducing fraud in organizations through information security policy compliance: An information security controls perspective. Computers & Security, 144, 103958. DOI: <https://doi.org/10.1016/j.cose.2024.103958>

- BRĂSLAȘU, I., ANDRONESCU, A. y NĂSTAC, D. (2023). Easy to Remember, Hard to Guess: A Password Generation Tool for the Digital Age. *International Conference on Cybersecurity and Cybercrime*, 10, págs. 113-119. doi:<https://www.ceeol.com/search/chapter-detail?id=1123471>
- Bu, S. y Kim, H. (2022). Optimized URL feature selection based on genetic-algorithm-embedded deep learning for phishing website detection. *Electronics*, 11(7), 1090.
- Chang, S., Lu, H., Kumar, A. y Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*.
- Chen, S., Fan, L., Meng, G., Su, T., Xue, M., Xue, Y., ... & Xu, L. (2020, June). An empirical assessment of security risks of global android banking apps. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (pp. 1310-1322).
- Chen, Z., Wu, L., Hu, Y., Cheng, J., Hu, Y., Zhou, Y. y Ren, K. (2024). Lifting the Grey Curtain: Analyzing the Ecosystem of Android Scam Apps. *IEEE Transactions on Dependable and Secure Computing*, 21(4), 3406-3421. doi:<https://doi.org/10.1109/TDSC.2023.3329205>
- Ciechanowski, L., Przegalinska, A., Magnuski, M., & Gloor, P. (2019). In the shades of the uncanny valley: An experimental study of human–chatbot interaction. *Future Generation Computer Systems*, 92, 539–548. <https://doi.org/10.1016/j.future.2018.01.055>
- Cordero, Z. (2009). La Investigación aplicada: Una forma de conocer las realidades con evidencia científica. *Revista Educación*, 33(1), 155–165. <https://doi.org/10.15517/REVEDU.V33I1.538>
- Danish, M. y Herrera, F. (2024). Legal and Ethical Challenges of Implementing Cybersecurity Principles. *Human Resources Practices*. doi:10.13140/RG.2.2.12757.03047

- Dion, M. (2011). Corruption, fraud and cybercrime as dehumanizing phenomena. *International Journal of Social Economics*, 38(5), 466-476. doi:10.1108/03068291111123156
- Dix, A., Finlay, J., Abowd, G. y Beale, R. (2004). *Human-Computer Interaction*. Pearson Education Limited. Obtenido de https://paragnachaliya.in/wp-content/uploads/2017/08/HCI_Alan_Dix.pdf
- Ejaz, A., Mian, A. y Manzoor, S. (2023). Life-long phishing attack detection using continual learning. *Scientific Reports*, 13(1), 11488. doi:<https://doi.org/10.1038/s41598-023-37552-9>
- Estrela, P. M. A. B., Albuquerque, R. de O., Amaral, D. M., Giozza, W. F., & de Sousa Júnior, R. T. (2021). *A Framework for Continuous Authentication Based on Touch Dynamics Biometrics for Mobile Banking Applications*. *Sensors*, 21(12), 4212. <https://doi.org/10.3390/s21124212>
- Ekeh, G. E., Afolabi, Y. I., Uche-Nwachi, E. O., Ekeh, L. K., & Eze-Udu, E. (2022). Awareness of BVN, SIM swap and clone frauds: Methods and controls. *Science World Journal*, 17(2), 200-206. ISSN: 1597-6343
- Elsadig, M., Ibrahim, A., Basheer, S., Alohal, M., Alshunaifi, S., Alqahtani, H. y Nagmeldin, W. (2022). Intelligent deep machine learning cyber phishing url detection based on bert features extraction. *Electronics*, 11(22), 3647. doi:<https://doi.org/10.3390/electronics11223647>
- Fernández, A. V., & Rodríguez, J. M. C. (2017). Análisis de las ciberamenazas. *Cuadernos de estrategia*, (185), 97-138.
- García-Treviño, C. J., Pérez-Díaz, J. A., Vargas-Rosales, C., & Zareei, M. (2024). *Transparent multifactor authentication algorithm based on geolocation*. *IEEE Access*, 12, 84691–84705. <https://doi.org/10.1109/ACCESS.2024.3412691>

- Gezer, A., Warner, G., Wilson, C. y Shrestha, P. (2019). A flow-based approach for Trickbot banking trojan detection. *Computers y Security*, 84, 179-192. doi:<https://doi.org/10.1016/j.cose.2019.03.013>
- Ghourabi, A., Mahmood, M. A. y Alzubi, Q. M. (2020). A hybrid CNN-LSTM model for SMS spam detection in arabic and english messages. *Future Internet*, 12(9), 156. doi:<https://doi.org/10.3390/fi12090156>
- Giffary, R. y Ramadhani, E. (2022). Implementasi Bcrypt dengan SHA-256 pada Password Pengguna Aplikasi Golek Kost. *Jurnal Sistem Komputer dan Informatika (JSON)*, 3(4), 543-546. doi:<http://dx.doi.org/10.30865/json.v3i4.4285>
- González-Estrada, E., & Cosmes, W. (2019). Shapiro–Wilk test for skew normal distributions based on data transformations. *Journal of Statistical Computation and Simulation*, 89(17), 3258-3272.
- Gualberto, E., De Sousa, R., Thiago, P., Da Costa, J. y Duque, C. G. (2020). From feature engineering and topics models to enhanced prediction rates in phishing detection. *Ieee Access*, 8, 76368-76385. doi:<https://doi.org/10.1109/ACCESS.2020.2989126>
- Gupta, G. P., & Kulariya, M. (2016). A framework for fast and efficient cyber security network intrusion detection using Apache Spark. *Procedia Computer Science*, 93, 824–831. <https://doi.org/10.1016/j.procs.2016.07.238>
- Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. *Frontiers in big Data*, 4, 583723
- Hagendorff, T. (2020). The ethics of AI ethics: An evaluation of guidelines. *Minds and machines*, 30(1), 99-120. doi:10.1007/s11023-020-09517-8
- Hansford, G. y Peltier, A. (2018). *Handbook of Information Security Management* (6 ed., Vol. 2). Auerbach Publications.

- Hassan, M. y Shukur, Z. (2021). Device identity-based user authentication on electronic payment system for secure E-wallet apps. *Electronics*, 11(4), 4. doi:<https://doi.org/10.3390/electronics11010004>
- Hassan, M. A., & Shukur, Z. (2022). *Device identity-based user authentication on electronic payment system for secure e-wallet apps*. *Electronics*, 11(1), 4. <https://doi.org/10.3390/electronics11010004>
- Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2021). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (7.^a ed.). McGraw-Hill Education
- Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications*, 193, 116429. DOI : <https://doi.org/10.1016/j.eswa.2021.116429>
- Holt, T.(2019). *The human factor of cybercrime*. Routledge.
- Ikhsan, R. B., Fernando, Y., Prabowo, H., Yuniarty, A., & Gui, A. (2024). An empirical study on the use of artificial intelligence in the banking sector of Indonesia by extending the TAM model and the moderating effect of perceived trust. *Digital Business*, 5, 100103. <https://doi.org/10.1016/j.digbus.2024.100103>
- Kala, N. (2021). Assessment of SIMBox Fraud: An Approach to National Security Threat. *Innovations in Science and Technology*. doi:<https://doi.org/10.9734/bpi/ist/v1/12787D>
- Kalabarige, L., Rao, R., Abraham, A. y Gabralla, L. (2022). Multilayer stacked ensemble learning model to detect phishing websites. *IEEE Access*, 10, 79543-79552. doi:<https://doi.org/10.1109/ACCESS.2022.3194672>
- Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, vol. 33, no 2004, p. 1-26
- Khan, H. U., Sohail, M., Nazir, S., Hussain, T., Shah, B., & Ali, F. (2023). *Role of authentication factors in Fin-tech mobile transaction security*. *Journal of Big Data*, 10(138). <https://doi.org/10.1186/s40537-023-00807-3>

- Khalili, N. (2022). Design and Implementation of a Blockchain-based Global Authentication System Using Biometrics and Subscriber Identification Module. Canada: Université d'Ottawa/University of Ottawa. doi:<http://dx.doi.org/10.20381/ruor-27891>
- Kerlinger, F. N., & Lee, H. B. (2002). *Foundations of behavioral research* (4.^a ed.). Wadsworth.
- Kim, M., Suh, J. y Kwon, H. (2022). A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures. IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD). Danang. doi:<https://doi.org/10.1109/BCD54882.2022.9900510>
- Kisore, N. y Sagi, S. (2015). A secure SMS protocol for implementing digital cash system. In 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), (págs. 1883-1892). doi:<https://doi.org/10.1109/ICACCI.2015.7275893>
- Kuttiyappan, D., & Rajasekar, V. (2023). Improving the cyber security over banking sector by detecting the malicious attacks using the wrapper stepwise ResNet classifier. *KSII Transactions on Internet and Information Systems*, 17(1), 515-527. <https://doi.org/10.3837/tiis.2023.01.027>
- Lafuente, C., & Egoscózábal, A. (2008). Metodologías de la investigación en las ciencias sociales: Fases, fuentes y selección de técnicas. *Escuela de Administración de Negocio (EAN)*, 64(1), 5-8. <https://www.redalyc.org/pdf/206/20612981002.pdf>
- Liu, X. y Fu, J. (2020). SPWalk: Similar property oriented feature learning for phishing detection. *Ieee Access*, 8, 87031-87045. doi:10.1109/ACCESS.2020.2992381
- Liu, B., Zhang, C., Yao, L., & Xin, Y. (2023). *GLPS: A Geohash-Based Location Privacy Protection Scheme*. *Entropy*, 25(12), 1569. <https://doi.org/10.3390/e25121569>

- Liu, X., Du, X., Zhang, X., Zhu, Q., Wang, H. y Guizani, M. (2019). Adversarial samples on android malware detection systems for IoT systems. *Sensors*, 19(4), 974. doi:<https://doi.org/10.3390/s19040974>
- Lien, C.-W., & Vhaduri, S. (2023). *Challenges and opportunities of biometric user authentication in the age of IoT: A survey*. *ACM Computing Surveys*, 56(1), Article 14, 37 páginas. <https://doi.org/10.1145/3603705>
- López, J., y García, F. (2021). Implementación de modelos de seguridad para dispositivos IoT en el sector financiero. *Revista de Innovación Tecnológica*, 13(2), 22-37.
- Machicado, J. (2010). Concepto de delito (Vol. 6). Apuntes jurídicos. Obtenido de <https://ermoquisbert.tripod.com/pdfs/concepto-delito.pdf>
- Macnish, K. y Van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in society*, 63, 101382. doi:<https://doi.org/10.1016/j.techsoc.2020.101382>
- Mambina, I., Ndibwile, J. y Michael, K. (2022). Classifying swahili smishing attacks for mobile money users: A machine-learning approach. *IEEE Access*, 10, 83061-83074. doi:<https://doi.org/10.1109/ACCESS.2022.3196464>
- Mathew, A. (2022). Threats and protection on E-sim: a prospective study. *Novel Persp. of Eng. Research*, 8, 76-81. doi:<https://doi.org/10.9734/bpi/rtcams/v8/1907B>
- McBride, G. G. (2008). Integrated Threat Management. En H. F. Tipton y M. Krause (Eds.), *Information Security Management Handbook* (6a ed., Vol. 2, pp. 3-13). Auerbach Publications.
- Medina, M. et al. (2023). *Metodología de la investigación: Técnicas e instrumentos de investigación*. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú.
- Mejía, D., y Azar, K. (2021). Políticas de inclusión financiera y las nuevas tecnologías en América Latina. Corporación Andina de Fomento (CAF). <https://scioteca.caf.com>

- México, B. (2024). BBVA México. Obtenido de <https://www.bbva.mx/educacion-financiera/banca-digital/cuenta-digital-fraude-cibernetico.html>
- Mishra, S. y Soni, D. (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, 108, 803-815. doi:<https://doi.org/10.1016/j.future.2020.03.021>
- Mitnick, K. y Vamosi, R. (2002). *The Art of Deception: Controlling the Human Element in Security*. Wiley Publishing Inc.
- Moedjahedy, J., Setyanto, A., Alarfaj, F. y Alreshoodi, M. (2022). CCrFS: combine correlation features selection for detecting phishing websites using machine learning. *Future Internet*, 14(8), 229. doi:<https://doi.org/10.3390/fi14080229>
- Mohamed, G., Visumathi, J., Mahdal, M., Anand, J. y Elangovan, M. (2022). An effective and secure mechanism for phishing attacks using a machine learning approach. *Processes*, 10(7), 1356. doi:<https://doi.org/10.3390/pr10071356>
- Monda, N. (2020). Assessment of technological risks facing mobile banking: a case of commercial banks in Kenya. Doctoral dissertation. Africa: Africa Nazarene University. Obtenido de <https://repository.anu.ac.ke/handle/123456789/597>
- Mongay Batalla, J. (2024). Featured papers on network security and privacy. *Journal of Sensor and Actuator Networks*, 13(11). <https://doi.org/10.3390/jsan13010011>
- Moreno-Hernandez, J., Campos-Molano, J., Medina-Betancourt, Y., y Poloche-Valencia, D. (2023). La inteligencia artificial como herramienta para la detección del fraude fiscal: Caso Colombia. *Revista Económica*, 11(2), 25-28. <https://doi.org/10.54753/rve.v11i2.1677>
- Nieto Rodríguez, C. O., y Sánchez Rojas, A. L. (2023). Riesgos cibernéticos en el sector financiero colombiano: Situación actual y tendencias. [Trabajo de grado, Fundación Universitaria del Área Andina].
- Organización de los Estados Americanos. (2018). Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe. <https://scioteca.oas.org>

- Panaqué Domínguez, J. A., Lizárraga Caipo, Y. G., y Mendoza de los Santos, A. (2022). Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones. *Perfiles de Ingeniería*, 18, 67-76. https://doi.org/10.31381/perfiles_ingenieria.v18i18.5399
- Panda, P., Mishra, A. y Puthal, D. (2022). A novel logo identification technique for logo-based phishing detection in cyber-physical systems. *Future Internet*, 14(8), 241. doi:<https://doi.org/10.3390/fi14080241>
- Park, H. y Sangjin, L. (2023). Countermeasures against ‘SIM-Swapping’ Crime through Criminal Script Analysis. *Revista de Investigación Criminal*, 9(1), 87-110. doi:10.46225/cis.2023.04.9.1.87
- Pérez, A., y Rodríguez, J. (2020). Estrategias de seguridad informática en bancos latinoamericanos frente a amenazas emergentes. [Tesis de Maestría, Universidad Nacional Autónoma de México].
- Prayogi, A. y Aji, R. (2023). Utilization of Mobile Network Infrastructure to Prevent Financial Mobile Application Account Takeover. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 797-808. doi:<https://doi.org/10.29207/resti.v7i4.5025>
- Qi, Q., Wang, Z., Xu, Y., Fang, Y. y Wang, C. (2023). Enhancing Phishing Email Detection through Ensemble Learning and Undersampling. *Applied Sciences*, 13(15), 8756. doi:<https://doi.org/10.3390/app13158756>
- Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, 23(3), 383-404.
- Rahman, M., Timko, D., Wali, H. y Neupane, A. (2023). Users Really Do Respond To Smishing. *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, (págs. 49-60). doi:10.1145/3577923.3583640

- Robbins, S. (2019). A misdirected principle with a catch: explicability for AI. *Minds and Machines*, 29(4), 495-514. doi:10.1007/s11023-019-09509-3
- Roy, S., Awad, A., Amare, L., Erkihun, M. y Anas, M. (2022). Multimodel phishing url detection using lstm, bidirectional lstm, and gru models. *Future Internet*, 14(11), 340. doi:<https://doi.org/10.3390/fi14110340>
- Shah, P., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information & Computer Security*, 28(2), 293-318.
- Sahingoz, O., Buber, E., Demir, O. y Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, 117, 345-357. doi:<https://doi.org/10.1016/j.eswa.2018.09.029>
- Saint-Pierre, H. (2008). Defensa y seguridad. En *Atlas Comparativo de la Defensa en América Latina*. RESDAL (Red de Seguridad y Defensa de América Latina). Obtenido de <http://www.cedoh.org/proyectos/FFAA/downloads/lecturas/files/defensa.pdf>
- Saldaña, M. R. (2016). Pruebas de bondad de ajuste a una distribución normal. *Revista Enfermería del trabajo*, 6(3), 114.
- Sauro, J., & Lewis, J. R. (2016). *Quantifying the user experience: Practical statistics for user research*. Morgan Kaufmann.
- Sathya, R., Kiran, U., Chowdary, J. y Kumar, B. (2020). Detection of Phishing Attacks using Random Forest Algorithm. *International Journal of Advanced Science and Technology*, 29(6), 6483-6490. Obtenido de <http://sersc.org/journals/index.php/IJAST/article/view/20095>
- Seth, P. y Madhavi, D. (2022). A Comprehensive Study of Classification of Phishing Attacks with its AI/I Detection. *International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)*, 370-375. doi:10.1109/IIHC55949.2022.10060305

- Sharma, G., & Ghosh, M. (2021). A secure lightweight authentication protocol for mobile payment. En *Advances in Cyber Security: Principles, Techniques, and Applications* (pp. 515-527). Springer. https://doi.org/10.1007/978-981-15-9774-9_48
- Shaukat, M., Amin, R., Muslam, M., Alshehri, A. y Xie, J. (2023). A hybrid approach for alluring ads phishing attack detection using machine learning. *Sensors*, 23(19), 8070. doi:<https://doi.org/10.3390/s23198070>
- Soi, D., Sanna, A., Maiorca, D., y Giacinto, G. (2024). Enhancing android malware detection explainability through function call graph APIs. *Journal of Information Security and Applications*, 80, 103691.
- Sonowal, G. (2020). Detecting phishing SMS based on multiple correlation algorithms. *SN computer science*, 1(6), 361. doi:<https://doi.org/10.1007/s42979-020-00377-8>
- Sonowal, G. (2020). Phishing email detection based on binary search feature selection. *SN Computer Science*, 1(4), 191. doi:<https://doi.org/10.1007/s42979-020-00194-z>
- Su, M. y Su, K. (2023). BERT-based approaches to identifying malicious URLs. *Sensors*, 23(8499). <https://doi.org/10.3390/s23208499>
- Sutherland, E. (1958). *The Sutherland Papers* (Vol. 36). Social Forces.
- Talavera Álvarez, V. R. (2015). Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. [Tesis de grado, Pontificia Universidad Católica del Perú].
- Tang, C., Chen, S., Fan, L., Xu, L., Liu, Y., Tang, Z. y Dou, L. (2019). A large-scale empirical study on industrial Fake Apps. *IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, 183-192. doi:<https://doi.org/10.1109/ICSE-SEIP.2019.00028>

- Timko, D. y Rahman, M. (2023). Commercial Anti-Smishing Tools and Their Comparative Effectiveness Against Modern Threat. *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, (págs. 1-12). doi:10.1145/3558482.3590173
- Ullah, F., Al-Turjman, F. y Nayyar, A. (2020). IoT-based green city architecture using secured and sustainable android services. *Environmental Technology y Innovation*, 20, 101091. doi:<https://doi.org/10.1016/j.eti.2020.101091>
- Ullah, F., Naeem, M., Mostarda, L. y Shah, S. (2021). Clone detection in 5G-enabled social IoT system using graph semantics and deep learning model. *International Journal of Machine Learning and Cybernetics*, 12, 3115-3127. doi:<https://doi.org/10.1007/s13042-020-01246-9>
- Ulqinaku, E., Stefa, J., & Mei, A. (2019, April). Scan-and-pay on android is dangerous. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1-6). IEEE.
- Valladares-Albarracín, J. J., y Ordóñez-Parra, Y. L. (2024). La aplicación de inteligencia artificial en la auditoría contable. *Revista Multidisciplinaria Perspectivas Investigativas*, 4(Contabilidad y Auditoría II), 73-85. <https://doi.org/10.62574/rmpi.v4iespecial.172>
- Wang, H., Liu, Z., Liang, J., Vallina-Rodriguez, N., Guo, Y., Li, L. y Xu, G. (2018). Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets. *IMC '18: Proceedings of the Internet Measurement Conference 2018* (págs. 293 - 307). New York: Association for Computing Machinery. doi:<https://doi.org/10.1145/3278532.3278558>
- Whitman, M. y Mattord, H. (2017). *Management of Information Security* (5 ed.). Cengage.
- Xia, P., Wang, H., Zhang, B., Ji, R., Wu, L., Luo, X. y Xu, G. (2020). Characterizing cryptocurrency exchange scams,. *Computers y Security*, 98, 101993. doi:<https://doi.org/10.1016/j.cose.2020.101993>

- Xie, J. yan, X., Lin, Y. y Wei, J. (2021). An accurate and efficient two-phase scheme for detecting Android cloned applications. *Concurrency and Computation: Practice and Experience*, 33(5). doi:<https://doi.org/10.1002/cpe.6009>
- Zambrano Loaiza, A. C., & Suárez Castro, J. C. (2020). La seguridad de las aplicaciones bancarias y dispositivos sin soporte oficial: Un análisis de riesgos. *Universidad Militar Nueva Granada*.
<https://repository.unimilitar.edu.co/bitstream/handle/10654/36702/ZambranoLoaizaAngieCarolina-SuarezCastroJohanCamilo2020.pdf?isAllowed=y&sequence=1>
- Zhang, L. yang, Z., He, Y., Li, M. yang, S. yang, M. y Qian, Z. (2019). App in the Middle: Demystify Application Virtualization in Android and its Security Threats. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 3(1), 1-24. doi:
<https://doi.org/10.1145/3322205.3311088>
- Zukarnain, Z. A., Muneer, A., & Ab Aziz, M. K. (2022). *Authentication securing methods for mobile identity: Issues, solutions and challenges*. *Symmetry*, 14(4), 821. <https://doi.org/10.3390/sym14040821>
- Statcounter Global Stats. (2025, julio). *Mobile Operating System Market Share Worldwide*. Statcounter. <https://gs.statcounter.com/os-market-share/mobile/worldwide>

ANEXOS

Anexo 1: Glosario de términos

Sección 1: Seguridad Informática y Fraude Cibernético

1. **Seguridad de la Información:** Conjunto de políticas y medidas para proteger la información digital de accesos no autorizados, ataques o alteraciones.
2. **Ciberdelincuencia:** Actividades delictivas cometidas mediante el uso de computadoras y redes, incluyendo fraudes, robo de identidad y ataques a sistemas informáticos.
3. **Hacking:** Proceso de explorar y explotar vulnerabilidades en sistemas informáticos para obtener acceso no autorizado o comprometer datos.
4. **Fraude Informático:** Delitos que implican el uso de tecnología informática para cometer fraude, como el robo de información confidencial o financiera.
5. **Phishing:** Ataque cibernético que busca engañar a los usuarios haciéndose pasar por una entidad confiable para obtener información personal y financiera.
6. **Spoofing:** Técnica en la que un atacante falsifica su identidad para engañar a un sistema o a un usuario, común en fraudes electrónicos.
7. **SIM Swapping:** Técnica fraudulenta en la que un ciberdelincuente clona o duplica la tarjeta SIM de la víctima para interceptar códigos de autenticación y tomar control de cuentas.

Sección 2: Autenticación y Protección en Aplicaciones Móviles

8. **OTP (One-Time Password):** Contraseña de un solo uso, enviada al dispositivo del usuario para validar la autenticidad de una transacción o acceso.
9. **IMEI (International Mobile Equipment Identity):** Número de identificación único para cada dispositivo móvil, utilizado en la autenticación de seguridad en las aplicaciones.
10. **Huella Dactilar:** Tecnología de autenticación biométrica que utiliza las características únicas de la huella dactilar del usuario para verificar su identidad.
11. **Aplicación Falsa (Fake App):** Programa malicioso diseñado para parecer legítimo, con el fin de acceder y manipular datos del dispositivo o realizar operaciones fraudulentas.

- 12. **Geolocalización:** Herramienta de seguridad que utiliza la ubicación del dispositivo móvil para verificar la autenticidad de transacciones y prevenir fraudes.
- 13. **Token Digital (OTP Token):** Código generado por una aplicación o dispositivo de seguridad que permite verificar la identidad del usuario durante una transacción.
- 14. **Smishing:** Tipo de fraude en el que se utilizan mensajes SMS para engañar a los usuarios y obtener información personal o financiera.
- 15. **Vishing:** Variante del phishing en la que se utilizan llamadas telefónicas para engañar a la víctima y obtener datos confidenciales, como contraseñas o información bancaria.

Sección 3: Herramientas y Técnicas de Ciberseguridad

- 16. **Fuerza Bruta:** Método de ataque en el que se prueban múltiples combinaciones de contraseñas hasta encontrar la correcta, utilizando herramientas automatizadas.
- 17. **Reconocimiento de IMEI:** Proceso de identificación y verificación del IMEI de un dispositivo como parte de una estrategia de seguridad.
- 18. **Cifrado de Datos:** Técnica que transforma datos legibles en un formato codificado para proteger la información de accesos no autorizados.
- 19. **Firewall:** Sistema de seguridad que controla el tráfico entrante y saliente de una red para protegerla de accesos no autorizados y amenazas cibernéticas.
- 20. **Antivirus:** Programa diseñado para detectar, prevenir y eliminar software malicioso, como virus, troyanos y otros tipos de malware.

Anexo 2: Estadística referente a cifras de Ciberseguridad en el mundo

Carpeta de reportes: [REPORTES DE CIBERSEGURIDAD](#)

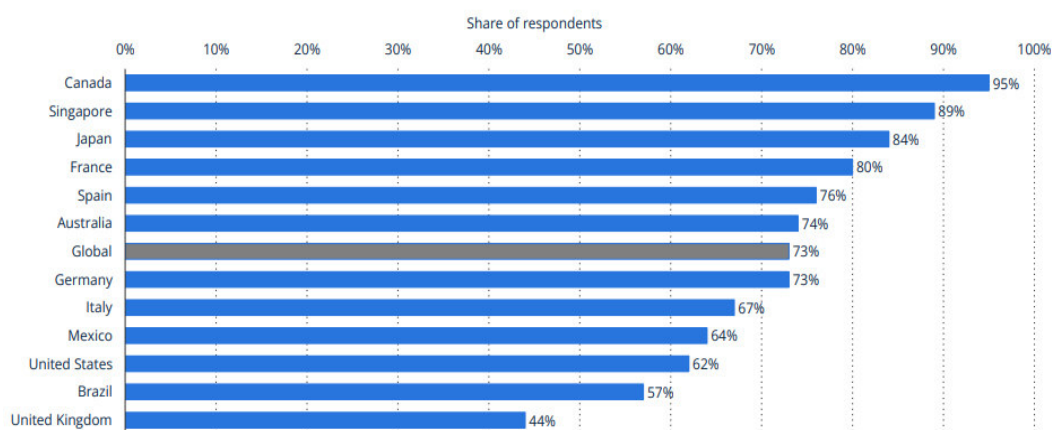
Figura 26

Reporte de Ciberseguridad en América Latina y el Caribe



Figura 27

Estadísticas referentes a la vulnerabilidad de países a ciber ataques



Description: According to a 2023 survey among board members of worldwide organizations, approximately 95 percent of companies in Canada were at risk of a material cyberattack. The majority of board members in Singapore, 89 percent, thought their companies were at such risk within the following 12 months. Japanese companies ranked third, with 84 percent of board members seeing a risk of a material cyber attack in the next year. [Read more](#)

Note: Worldwide, June 9 to 16, 2023; board directors; expected attacks in the next 12 months

Source: Statista, Proton

statista

Figura 28
Proyección del valor del mercado mundial de la ciberseguridad al 2023

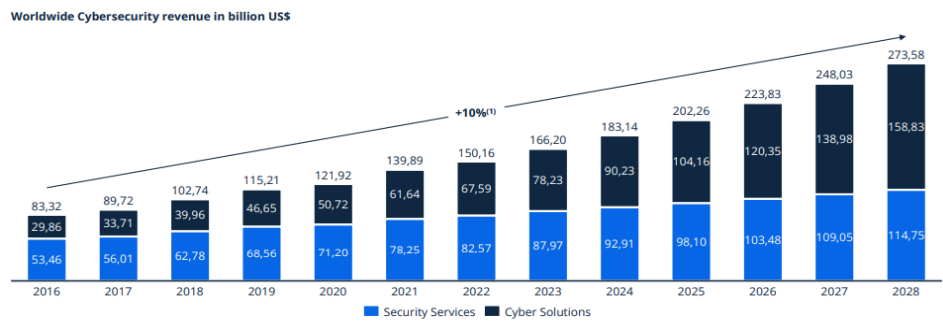


Figura 29
Ingresos del mercado de la ciberseguridad en la región de Asia y el Pacífico desde 2017 hasta 2022, con previsiones hasta 2026

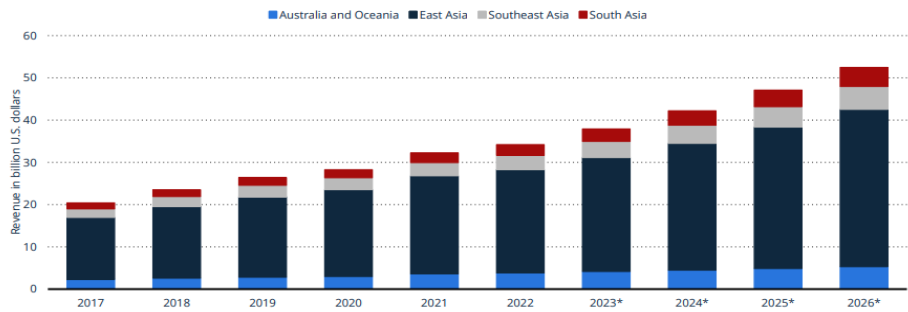
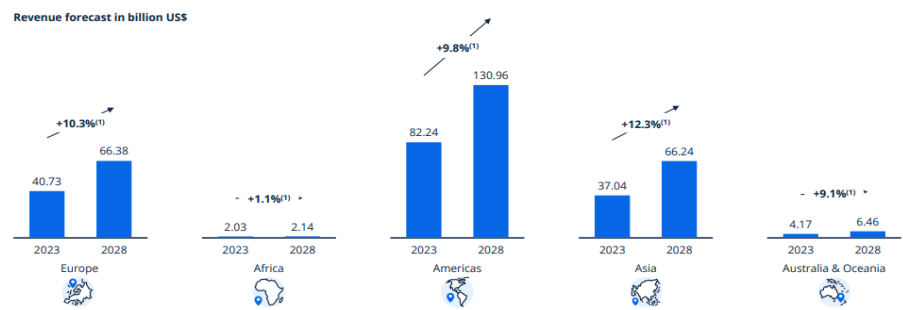


Figura 30
América es el mercado más grande entre las regiones seleccionadas en 2023



Anexo 3: Formulario para las personas que usaron el Modelo Sectrabank.

1. Ingrese su correo personal
2. Ingrese su correo institucional
3. Según el grupo generacional, indique su edad.
4. Género:
5. Procedencia:
6. Marca del equipo telefónico que utiliza
7. ¿Usted realiza operaciones bancarias?
8. ¿Tienes conocimiento de los ataques de fraude Informático en la modalidad de Fake App y Sim Swapping?
9. Usted, su entorno amical o familiar, ¿En alguna oportunidad ha sido víctima de fraude informático?
10. Si su respuesta es afirmativa, indique el vínculo con la víctima.
11. Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular.
12. ¿Consideras que el modelo propuesto ha mitigado el ataque simulado de Fake App ejecutado en su dispositivo móvil?
13. ¿Consideras que el modelo propuesto ha mitigado el ataque simulado de SIM Swapping ejecutado en su dispositivo móvil?
14. Usted estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de Fake App y SIM Swapping.

Enlace al Formulario Virtual: <https://forms.gle/Q4T2PnkqsQcVWN6J6>

Anexo 4: Respuestas recopiladas en el formulario

A. Grupo Control

Ingrese su correo personal	Ingrese su correo institucional	Según el grupo generacional, indique su edad	Género	Procedencia	¿Tiene conocimiento de los ataques de fraude informático en la modalidad de Fake App y Sim Swap?	¿Usted realizó alguna operación bancaria?	¿Tiene conocimiento de los ataques de fraude informático en la modalidad de Fake App y Sim Swap?	¿En alguna oportunidad ha sido víctima de fraude informático?	Si su respuesta es afirmativa, indique el vínculo con la víctima	Si su respuesta es afirmativa, indique el vínculo con la víctima	Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular	¿Modelo propuesto ha mitigado el ataque simulado de Fake App ejecutado en su dispositivo móvil?	¿Modelo propuesto ha mitigado el ataque simulado de SIM Swapping ejecutado en su dispositivo móvil?	¿Usted estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?
lencaschevarria@gmail.com	lencaschevarria@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No, es amigable, pero no evitó que mi app fuera infectada.	No	No	No
ylfadatshuanan@gmail.com	ylfadatshuanan@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	Sí	Si familiar	La navegación es clara, pero no es efectiva en detectar fraudes.	No	No	No	No	No
camana11@gmail.com	camana11@gmail.com	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMSM Samsung	Sí	Sí	No	No	No	No	No	No	No	No
romero d9@gmail.com	romero d9@gmail.com	Millennials (27 a 38)	Femenino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	No	No	No	No	No	No	No	No
sove.1995@gmail.com	sove.1995@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
valata@unmsm.edu.pe	valata@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	No	Si familiar	No, el diseño es bueno, pero no me protegí contra la Fake App.	No	No	No	No	No
1400@hotmail.com	1400@hotmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	No	No	No	No	No	No	No	No
u1024@hotmail.com	u1024@hotmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
harez70@gmail.com	harez70@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	No	No	No	No	No	No	No	No
avila.ade@gmail.com	avila.ade@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	Sí	Si familiar	La aplicación es sencilla, pero permitió la infección.	No	No	No	No	No
xe1555@gmail.com	xe1555@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Samsung	Sí	Sí	No	No	No	No	No	No	No	No
uuoutlook.com	uuoutlook.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Huawei	Sí	Sí	No	Si persona	No, funciona bien, pero no detectó actividad sospechosa.	Sí	Sí	Sí	Sí	Sí
stiven4@gmail.com	stiven4@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	Sí	Si familiar	No, es amigable, pero no bloqueó la amenaza a tiempo.	No	No	No	No	No
alo@unmsm.edu.pe	alo@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	Sí	Si familiar	Es clara y ordenada, pero falló en la prevención.	No	No	No	No	No
zaveleta@unmsm.edu.pe	zaveleta@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Poo	Sí	Sí	No	No	No	No	No	No	No	No
nvalidia@unmsm.edu.pe	nvalidia@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
aldivia@unmsm.edu.pe	aldivia@unmsm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Honor	Sí	Sí	Sí	Si familiar	No, me pareció rápida, pero mi app fue clonada.	No	No	No	No	No
unmsm.edu.pe	unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	No	No	No	No	No	No	No	No
avienzo@unmsm.edu.pe	avienzo@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	Sí	Si persona	No, los menús son comprensibles, pero no impidió el ataque.	No	No	No	No	No
calero@unmsm.edu.pe	calero@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Samsung	Sí	Sí	No	No	No	No	No	No	No	No
lin.espiroz@unmsm.edu.pe	lin.espiroz@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
casimiro@unmsm.edu.pe	casimiro@unmsm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Huawei	Sí	Sí	Sí	Si persona	Me gustó la navegación, pero no protegí mis credenciales.	No	No	No	No	No
berrocal@unmsm.edu.pe	berrocal@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	No	No	No	No	No	No	No	No
tro.torres@unmsm.edu.pe	tro.torres@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
urbano@unmsm.edu.pe	urbano@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Huawei	Sí	Sí	No	No	No	No	No	No	No	No
aldivia@unmsm.edu.pe	aldivia@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Samsung	Sí	Sí	No	Si familiar	La navegación es lógica, pero no detectó la anomalía.	No	No	No	No	No
valer@unmsm.edu.pe	valer@unmsm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
re@unmsm.edu.pe	re@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Samsung	Sí	Sí	No	No	No	No	No	No	No	No
triga@unmsm.edu.pe	triga@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
villafrañca@unmsm.edu.pe	villafrañca@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	Sí	Si persona	El diseño es atractivo, pero no alertó sobre el ataque.	No	No	No	No	No
zaxarzas@unmsm.edu.pe	zaxarzas@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Huawei	Sí	Sí	No	No	No	No	No	No	No	No
tero@unmsm.edu.pe	tero@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	Sí	Si persona	Las opciones están bien organizadas, pero la seguridad no es efectiva.	No	No	No	No	No
huayamara@unmsm.edu.pe	huayamara@unmsm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMSM Samsung	Sí	Sí	No	No	No	No	No	No	No	No
yayanay@unmsm.edu.pe	yayanay@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
unmsm.edu.pe	unmsm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	No	No	No	No	No	No	No	No
htz@unmsm.edu.pe	htz@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Samsung	Sí	Sí	No	Si familiar	El diseño es atractivo, pero no alertó sobre el ataque.	No	No	No	No	No
achad@unmsm.edu.pe	achad@unmsm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
nie.perez@unmsm.edu.pe	nie.perez@unmsm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMSM Motorola	Sí	Sí	No	No	No	No	No	No	No	No
uinones@unmsm.edu.pe	uinones@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	Sí	Si familiar	No, tiene buena organización, pero no alertó sobre la Fake App.	No	No	No	No	No
a.seminario@unmsm.edu.pe	a.seminario@unmsm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMSM Samsung	Sí	Sí	No	No	No	No	No	No	No	No
villanueva@unmsm.edu.pe	villanueva@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Huawei	Sí	Sí	No	No	No	No	No	No	No	No
lvarez@unmsm.edu.pe	lvarez@unmsm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMSM Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No	No
anchez@gmail.com	anchez@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
alco@gmail.com	alco@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
nogotlon.flavila@gmail.com	nogotlon.flavila@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	Si familiar	El diseño es atractivo, pero no alertó sobre el ataque.	No	No	No	No	No
llype.romero@gmail.com	llype.romero@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
ris.salas@gmail.com	ris.salas@gmail.com	Millennials (27 a 38)	Femenino	Divinat PNP	Motorola	Sí	Sí	No	No	No	No	No	No	No
asta@gmail.com	asta@gmail.com	Millennials (27 a 38)	Femenino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
roz@gmail.com	roz@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Motorola	Sí	Sí	Si familiar	Me pareció fácil de usar, pero igual fui víctima del ataque.	No	No	No	No	No
quipe@gmail.com	quipe@gmail.com	Generación Z (17 a 26)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
laron@gmail.com	laron@gmail.com	Millennials (27 a 38)	Femenino	Divinat PNP	Motorola	Sí	Sí	No	No	No	No	No	No	No
mija@gmail.com	mija@gmail.com	Millennials (27 a 38)	Femenino	Divinat PNP	Xicami - Redmi	Sí	Sí	Si familiar	La aplicación responde bien, pero no detectó el fraude.	No	No	No	No	No
condori@gmail.com	condori@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
shvajandri@gmail.com	shvajandri@gmail.com	Generación Z (17 a 26)	Masculino	Divinat PNP	Huawei	Sí	Sí	Si persona	No, es fluida, pero no impidió la suplantación.	No	No	No	No	No
otrina@gmail.com	otrina@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	Si familiar	No, tiene un buen diseño, pero no detectó la anomalía.	No	No	No	No	No
coo@gmail.com	coo@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
do.catacora@gmail.com	do.catacora@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
vareze@gmail.com	vareze@gmail.com	Millennials (27 a 38)	Femenino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
utz.conteras@gmail.com	utz.conteras@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	Si persona	La funcionalidad es buena, pero permitió el acceso indebido.	No	No	No	No	No
duardo.cardenas@gmail.com	duardo.cardenas@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
felix@gmail.com	felix@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
ilauke@gmail.com	ilauke@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Huawei	Sí	Sí	No	No	No	No	No	No	No
layme@gmail.com	layme@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
ntachoue@gmail.com	ntachoue@gmail.com	Generación Z (17 a 26)	Masculino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
manani@gmail.com	manani@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Huawei	Sí	Sí	Si entorno amigable	La configuración es intuitiva, pero la seguridad es deficiente.	No	No	No	No	No
era@gmail.com	era@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
segura@gmail.com	segura@gmail.com	Millennials (27 a 38)	Femenino	Divinat PNP	Xicami - Redmi	Sí	Sí	Si persona	Me gustó su apariencia, pero no protege como debería.	No	No	No	No	No
eth.tejada@gmail.com	eth.tejada@gmail.com	Millennials (27 a 38)	Femenino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
monteza.v@gmail.com	monteza.v@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	Si persona	No, la experiencia fue cómoda, pero mi app se infectó igual.	No	No	No	No	No
go.cardenas@gmail.com	go.cardenas@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
marinez@gmail.com	marinez@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
baquerizo@gmail.com	baquerizo@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Poo	Sí	Sí	No	No	No	No	No	No	No
reyes.b@gmail.com	reyes.b@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
via.arzapalo@gmail.com	via.arzapalo@gmail.com	Generación Z (17 a 26)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	Si familiar	La interfaz es atractiva, pero la app falsa se instaló sin problemas.	No	No	No	No	No
nueda@gmail.com	nueda@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
ulipe@gmail.com	ulipe@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
uliga@gmail.com	uliga@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Motorola	Sí	Sí	No	No	No	No	No	No	No
tonio.bendezu@gmail.com	tonio.bendezu@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Motorola	Sí	Sí	Si entorno amigable	Se siente moderna, pero no hubo alertas tempranas.	Sí	Sí	Sí	Sí	Sí
seman.arias@gmail.com	seman.arias@gmail.com	Millennials (27 a 38)	Femenino	Divinat PNP	Samsung	Sí	Sí	No	No	No	No	No	No	No
rosales@gmail.com	rosales@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Xicami - Redmi	Sí	Sí	No	No	No	No	No	No	No
zaveleta@gmail.com	zaveleta@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Honor	Sí	Sí	Si familiar	No, la aplicación es segura, pero no previno la suplantación de identidad.	No	No	No	No	No
nf@gmail.com	nf@gmail.com	Generación Z (17 a 26)	Masculino	Divinat PNP	Motorola	Sí	Sí	No	No	No	No	No	No	No
					Xicami - Redmi	Sí	Sí	Si familiar	No, el acceso es rápido, pero la seguridad no cumplió su función.	No	No	No	No	No
									No, tiene buena organización, pero no alertó sobre la Fake App.	No	No	No	No	No
									No, el flujo de uso es claro, pero no impidió la vulneración.	No	No	No	No	No
									No, parece confiable.	Sí	Sí	Sí	Sí	Sí
									El OTP funciona bien, pero la seguridad general es débil.	No	No	No	No	No
									Las validaciones son simples, pero no detectó la anomalía.	No	No	No	No	No
									No, su diseño es atractivo, pero permitió el acceso fraudulento.	No	No	No	No	No
									No, el proceso de autenticación es cómodo, pero no evitó el fraude.	No	No	No	No	No
									Permite hacer transacciones fácilmente, pero no evitó el hackeo.	No	No	No	No	No
									No, se adapta bien al usuario, pero la seguridad no respondió bien.	No	No	No	No	No
									Las opciones de navegación son claras, pero el ataque pasó desapercibido.	No	No	No	No	No
									No, es intuitiva, pero los controles de seguridad no funcionaron.	No	No	No	No	No
									Me pareció fácil de usar, pero igual fui víctima del ataque.	No	No	No	No	No
									El acceso es ágil, pero no hubo protección ante la app maliciosa.	No	No	No	No	No
									Las opciones de seguridad parecen completas, pero no lo son.	No	No	No	No	No
									No, la aplicación responde bien, pero no detectó el fraude.	No	No	No	No	No
									No, es fluida, pero no impidió la suplantación.	No	No	No	No	No
									No, tiene un buen diseño, pero no detectó la anomalía.	No	No	No	No	No
									La funcionalidad es buena, pero permitió el acceso indebido.	No	No	No	No	No
									No, el flujo de uso es claro, pero no detectó el cambio de SIM.	No	No	No	No	No
				</										

B. Grupo Experimental

Ingrese su correo personal	Ingrese su correo institucional	Según el grupo generacional, indique	Genero	Procedencia:	Marca del equipo telefónico que utiliza	¿Usted realiza operaciones bancarias?	¿Tiene conocimiento de los ataques de fraude informático en la modalidad de Fake App y Sim Swap?	¿Usted su entorno amical o familiar, ¿En alguna oportunidad ha sido víctima de fraude informático?	Si su respuesta es afirmativa, indique el vínculo con la víctima	¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su dispositivo móvil?	¿Considera que el modelo propuesto ha mitigado el ataque simulado de Fake App Swapping ejecutado en su dispositivo móvil?	¿Considera que el modelo propuesto ha mitigado el ataque simulado de SIM Swapping y Fake App?	¿Usted estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?
pe@gmail.com	ilvegasy@unmm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
s704@gmail.com	rob_rivas@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
apipasa2002@gmail.com	huerta@unmm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
gmail.com	on_ventura@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
prym1@gmail.com	more@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
2001@gmail.com	rodriguez@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
hishua@gmail.com	leon@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Huawei	Si	Si	No	Si	Si	Si	Si	Si	Si
ecangelmanuel@gmail.com	l_angeles@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Motorola	Si	Si	No	Si	Si	Si	Si	Si	Si
hvaradmarco@gmail.com	hvaradmarco@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
mbillito@gmail.com	tambillo@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Huawei	Si	Si	Si	Si	Si	Si	Si	Si	Si
boladillon@gmail.com	boladillon@gmail.com	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
razaman11@gmail.com	arazaman2@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si	Si
el271254@gmail.com	luis salazar@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	Si	Si	Si	Si	Si	Si	Si
passa3@gmail.com	cesar calderon@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
icel@gmail.com	monso lazo@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
salinas45@gmail.com	salinas@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
220x@gmail.com	condonadon@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Poo	Si	Si	No	Si	Si	Si	Si	Si	Si
rosod45@gmail.com	an alonso@gmail.com	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
si@gmail.com	an ortiz1@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si	Si
ez1109@gmail.com	lopez@unmm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
adog@gmail.com	prado@unmm.edu.pe	Millennials (27 a 38)	Femenino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
59@gmail.com	echegun@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Motorola	Si	Si	No	Si	Si	Si	Si	Si	Si
jaya@gmail.com	haya@unmm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Motorola	Si	Si	Si	Si	Si	Si	Si	Si	Si
stellanos@unmm.edu.pe	stellanos@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
reno@unmm.edu.pe	arreno@unmm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	Si	Si	Si	Si	Si	Si	Si
soza@unmm.edu.pe	rendoza@unmm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Motorola	Si	Si	No	Si	Si	Si	Si	Si	Si
campes@unmm.edu.pe	campes@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
pesto@unmm.edu.pe	podesto@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Huawei	Si	Si	Si	Si	Si	Si	Si	Si	Si
armas@unmm.edu.pe	armas@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Honor	Si	Si	No	Si	Si	Si	Si	Si	Si
unmm.edu.pe	ayta@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Poo	Si	Si	No	Si	Si	Si	Si	Si	Si
nto@unmm.edu.pe	quinto@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si	Si
tos@unmm.edu.pe	harcoo@unmm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
uipasa@unmm.edu.pe	uipasa@unmm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
martinez@unmm.edu.pe	martinez@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
nillo@unmm.edu.pe	munillo@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si	Si
manrique@unmm.edu.pe	manrique@unmm.edu.pe	Millennials (27 a 38)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Motorola	Si	Si	No	Si	Si	Si	Si	Si	Si
tores@unmm.edu.pe	tores@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si	Si
ardon@unmm.edu.pe	ardon@unmm.edu.pe	Generación Z (17 a 26)	Femenino	Escuela de Ingeniería de Software FISI - UNMS Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si	Si
en@unmm.edu.pe	en@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Huawei	Si	Si	No	Si	Si	Si	Si	Si	Si
andro@unmm.edu.pe	leandro@unmm.edu.pe	Generación Z (17 a 26)	Masculino	Escuela de Ingeniería de Software FISI - UNMS Samsung	Si	Si	No	Si	Si	Si	Si	Si	Si
fuerte@gmail.com	policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Motorola	Si	Si	Si	Si	Si	Si	Si	Si
human@gmail.com	an@policia gob.pe	Millennials (27 a 38)	Femenino	Divinat PNP	Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si
es@gmail.com	policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si
ne nacionaldo@gmail.com	onaco@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Huawei	Si	No	Si	Si	Si	Si	Si	Si
noza@gmail.com	za@policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Samsung	Si	Si	Si	Si	Si	Si	Si	Si
rado.romani@gmail.com	edo@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Xiaomi - Poo	Si	Si	No	Si	Si	Si	Si	Si
lopez@gmail.com	policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si
ony bolafon@gmail.com	os@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Honor	Si	Si	Si	Si	Si	Si	Si	Si
ndhercoma@gmail.com	hercoma@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Motorola	Si	No	Si	Si	Si	Si	Si	Si
ila@gmail.com	la@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si
g@gmail.com	g@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Si	No	Si	Si	Si	Si	Si	Si
chavez@gmail.com	ez@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si
hos arenas@gmail.com	policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Huawei	Si	Si	Si	Si	Si	Si	Si	Si
lars @gmail.com	policia gob.pe	Millennials (27 a 38)	Femenino	Divinat PNP	Motorola	Si	No	Si	Si	Si	Si	Si	Si
no@gmail.com	policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	No	Si	Si	Si	Si	Si	Si
nos h@gmail.com	s@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Huawei	Si	No	Si	Si	Si	Si	Si	Si
j rojas@gmail.com	policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Si	Si	Si	Si	Si	Si	Si	Si
uentera@gmail.com	uentera@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si
es@gmail.com	s@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Si	Si	No	Si	Si	Si	Si	Si
na b@gmail.com	a@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	No	Si	Si	Si	Si	Si	Si
caranza@gmail.com	policia gob.pe	Millennials (27 a 38)	Femenino	Divinat PNP	Motorola	Si	Si	Si	Si	Si	Si	Si	Si
es p@gmail.com	a@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Huawei	Si	Si	Si	Si	Si	Si	Si	Si
os@gmail.com	policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	Si	No	Si	Si	Si	Si	Si
roe@gmail.com	e@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Si	No	Si	Si	Si	Si	Si	Si
loayza@gmail.com	za@policia gob.pe	Millennials (27 a 38)	Femenino	Divinat PNP	Xiaomi - Redmi	Si	No	Si	Si	Si	Si	Si	Si
mpfn gob.pe	as@mpfn gob.pe	Millennials (27 a 38)	Femenino	Divinat PNP	Samsung	Si	No	Si	Si	Si	Si	Si	Si
23@gmail.com	23@gmail.com	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Si	No	Si	Si	Si	Si	Si	Si
31@gmail.com	31@gmail.com	Generación Z (17 a 26)	Masculino	Divinat PNP	Honor	Si	Si	Si	Si	Si	Si	Si	Si
iano@gmail.com	342@policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Motorola	Si	No	Si	Si	Si	Si	Si	Si
anca29@gmail.com	391@policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Samsung	Si	Si	Si	Si	Si	Si	Si	Si
rio@gmail.com	399@policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Honor	Si	Si	Si	Si	Si	Si	Si	Si
riesz22@gmail.com	447@policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Samsung	Si	Si	Si	Si	Si	Si	Si	Si
19a@gmail.com	3819a@gmail.com	Generación Z (17 a 26)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si
huncamajavier@gmail.com	o@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Motorola	Si	No	Si	Si	Si	Si	Si	Si
erero28@gmail.com	policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Honor	Si	Si	Si	Si	Si	Si	Si	Si
er@gmail.com	policia gob.pe	Millennials (27 a 38)	Femenino	Divinat PNP	Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si
er@gmail.com	policia gob.pe	Generación Z (17 a 26)	Masculino	Divinat PNP	Xiaomi - Redmi	Si	Si	Si	Si	Si	Si	Si	Si
rujan@gmail.com	policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Samsung	Si	Si	Si	Si	Si	Si	Si	Si
ez@policia gob.pe	hdez@policia gob.pe	Generación X (39 a 54)	Masculino	Divinat PNP	Samsung	Si	No	Si	Si	Si	Si	Si	Si
12@hotmail.com	s@policia gob.pe	Millennials (27 a 38)	Masculino	Divinat PNP	Huawei	Si	No	No	No	No	No	No	No

Anexo 5: Informe del grupo control y experimental con respecto a la usabilidad de parte de los usuarios

Informe del grupo Control

En este informe se presentan las opiniones recabadas de los 80 participantes del **grupo control**, quienes instalaron y utilizaron la aplicación bancaria sin las medidas avanzadas de protección contra ataques de *Sim Swapping* y *Fake Apps*. La pregunta realizada fue:

¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular?

A continuación, se expone un análisis detallado de las respuestas de los participantes del grupo control, enfocándose en los aspectos de **usabilidad**, **seguridad** y **funcionalidad** de la aplicación, además de las **limitaciones** percibidas por los usuarios respecto a la protección contra ataques de **fraude**.

1. Usabilidad de la Aplicación

Las opiniones sobre la **usabilidad** de la aplicación en el grupo control fueron en su mayoría positivas, destacando que la aplicación es **fácil de usar** y **accesible**. Los participantes mencionaron que la **interfaz es clara y ordenada**, y que la **navegación es lógica y fluida**. Comentarios como “**es intuitiva y tiene buena organización**”, “**la interfaz es moderna**”, “**la aplicación es sencilla de usar**” fueron recurrentes en las respuestas.

Sin embargo, a pesar de la facilidad de uso, muchos participantes indicaron que la **usabilidad** no fue suficiente para garantizar la **seguridad** que esperaban. En varios comentarios, los usuarios mencionaron que, aunque la aplicación era fácil de manejar y las opciones de navegación eran claras, **la seguridad no cumplió su función**. Opiniones como “**me pareció práctica, pero fui víctima de un ataque**” y “**la**

aplicación es sencilla, pero permitió la infección” reflejan una desconexión entre la percepción positiva de la interfaz y las fallas en la protección ante ataques externos.

2. Seguridad y Protección

La **seguridad** fue el aspecto más negativo en las respuestas del grupo control. A pesar de que muchos participantes elogiaron la **facilidad de uso** y la **accesibilidad** de la aplicación, la mayoría de las respuestas indicaron que la **protección contra fraudes** fue **insuficiente**. Las opiniones fueron consistentes en señalar que, aunque la aplicación parecía segura en apariencia, no logró evitar ataques de *Sim Swapping* ni **Fake Apps**. Comentarios como **“es clara y ordenada, pero falló en la prevención”**, **“permitió el SIM Swapping”**, **“no detectó la Fake App”** y **“no reaccionó ante el ataque”** fueron bastante comunes.

La falta de detección de **actividades sospechosas** y la **falta de alertas** sobre aplicaciones maliciosas fueron mencionadas frecuentemente. Muchos usuarios indicaron que la aplicación **permitió la instalación de malware** o **la clonación de la aplicación**, lo que demuestra una falta de mecanismos robustos para la prevención de amenazas cibernéticas. Respuestas como **“mi app fue clonada”**, **“la aplicación no detectó actividad sospechosa”** y **“no bloqueó el ataque a tiempo”** refuerzan la percepción de que la seguridad de la aplicación en este grupo no fue efectiva.

A pesar de que la **autenticación OTP** y **autenticación por huella digital** fueron mencionadas como funcionalidades positivas, muchos usuarios indicaron que estas medidas de seguridad fueron **superadas por los ataques**. Los comentarios como **“el sistema de autenticación es bueno, pero fue vulnerado”** y **“la autenticación por huella no protegió mi cuenta”** sugieren que, aunque los mecanismos de protección eran funcionales, no fueron suficientes para impedir los accesos fraudulentos.

3. Interfaz y Diseño

El **diseño** de la aplicación en el grupo control fue generalmente calificado de manera positiva, con comentarios como “**el diseño es atractivo**”, “**la interfaz es moderna**” y “**es fácil de manejar**”. La mayoría de los participantes destacaron que la aplicación era **práctica y bien organizada**, lo que facilita la **realización de transacciones y navegación**. La estructura del menú fue considerada **sencilla y accesible**, permitiendo que las opciones fueran fáciles de encontrar.

Sin embargo, a pesar de las valoraciones positivas sobre el diseño, muchos participantes coincidieron en que el **diseño atractivo no fue suficiente para evitar ataques**. Opiniones como “**en apariencia es segura, pero no fue efectiva en mi caso**” y “**el diseño es bueno, pero no protegió mis datos**” evidencian una contradicción entre la **apariencia segura** de la aplicación y la falta de medidas de **protección efectiva**.

4. Confianza y Fiabilidad

En términos de **confianza**, los participantes del grupo control fueron escépticos sobre la **fiabilidad** de la aplicación. Aunque algunos usuarios mencionaron que la aplicación parecía **confiable y segura en apariencia**, los ataques de **SIM swapping** y **Fake Apps** que sufrieron generaron una **desconfianza** hacia el modelo de seguridad implementado. Comentarios como “**parece confiable, pero el malware pasó desapercibido**” y “**parece segura, pero permitió el acceso fraudulento**” reflejan esta desconexión entre la **percepción inicial** de confianza y la **experiencia real** de fraude.

Aunque algunos usuarios mencionaron que las funcionalidades de la aplicación eran **accesibles y fáciles de usar**, el hecho de que la **seguridad no funcionara correctamente** llevó a una sensación generalizada de que la aplicación **no cumplió con sus expectativas** en términos de protección. La sensación de **inseguridad** fue mayor en aquellos que experimentaron ataques reales, lo que resalta la importancia de una **protección efectiva** en aplicaciones bancarias.

5. Términos Comunes Relacionados con el Modelo de Seguridad

En las respuestas del grupo control, se identificaron varios términos y conceptos clave relacionados con los **problemas de seguridad** experimentados:

- **Sim Swapping:** Un ataque en el que el fraudulento cambia la tarjeta SIM del usuario para acceder a sus servicios de teléfono móvil y cuentas bancarias.
- **Fake Apps:** Aplicaciones maliciosas que se hacen pasar por aplicaciones legítimas con el objetivo de robar información personal y financiera.
- **OTP (One-Time Password):** Contraseña de un solo uso enviada al usuario para realizar una validación durante las transacciones o accesos.
- **Autenticación por huella digital:** Método biométrico de autenticación que utiliza la huella dactilar del usuario para verificar su identidad.
- **Malware:** Software malicioso diseñado para dañar, alterar o robar información del sistema del usuario.
- **Clonación de la aplicación:** Proceso fraudulento en el que se copia la aplicación legítima para engañar al usuario y acceder a sus datos.
- **Acceso no autorizado:** Intentos de acceder a la cuenta o dispositivo sin la debida autorización.
- **Filtración de datos:** Proceso en el cual la información personal o financiera del usuario es comprometida y expuesta a terceros no autorizados.

Conclusión

En resumen, las opiniones del grupo control reflejan una experiencia mayormente negativa en términos de **seguridad**, a pesar de una **buena usabilidad** y un **diseño atractivo**. Aunque los usuarios valoraron la **facilidad de uso** y la **navegación clara**, la **protección contra fraudes** fue insuficiente para prevenir los ataques de **Sim Swapping** y **Fake Apps**. La **autenticación** y las medidas de **seguridad**

en tiempo real no fueron suficientes para impedir el acceso no autorizado, lo que generó desconfianza en la fiabilidad del sistema.

La falta de una **detección temprana de amenazas**, así como la incapacidad para bloquear aplicaciones maliciosas, subraya las deficiencias de seguridad de la aplicación en este grupo. Esto destaca la importancia de reforzar los mecanismos de **protección contra fraudes** y mejorar la **efectividad de la detección de amenazas** para garantizar la seguridad de los usuarios.

Informe Grupo Experimental

En este informe se presentan las opiniones recabadas de los 80 participantes del grupo experimental que instalaron y utilizaron una aplicación bancaria diseñada con medidas de seguridad avanzadas, específicamente enfocada en la protección contra ataques de *Sim Swapping* y aplicaciones falsas (*Fake Apps*). La pregunta realizada fue:

¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular?

A continuación, se expone un análisis detallado de las respuestas de los participantes, abordando principalmente la **usabilidad** de la aplicación, las **funciones de seguridad** implementadas, el **diseño de la interfaz** y la **confianza** generada por la aplicación.

1. Usabilidad de la Aplicación

Una de las áreas más destacadas en las respuestas de los participantes fue la **usabilidad de la aplicación**, que fue calificada de manera muy positiva. La mayoría de los encuestados coincidió en que la aplicación es **amigable, fácil de usar e intuitiva**. Muchas respuestas destacaron que la interfaz es **clara y moderna**, lo que facilita la navegación y las operaciones dentro de la aplicación. Comentarios como “**la interfaz es clara y moderna**”, “**la navegación es fluida y sin complicaciones**” y “**la disposición de los menús facilita la navegación**” fueron comunes entre los participantes.

El hecho de que la aplicación se pueda utilizar fácilmente desde el primer uso también fue resaltado, con opiniones que mencionan que no fue necesario un aprendizaje largo para comprender cómo operar la aplicación. Además, muchos usuarios afirmaron que **la experiencia de usuario fue excelente**, lo que indica que la aplicación cumple con los estándares de facilidad de uso.

En términos de la interacción, los participantes señalaron que **la aplicación no presentó fallos** en su funcionamiento, lo que refuerza la idea de que es una herramienta

eficaz para realizar transacciones bancarias de manera sencilla y sin inconvenientes. A nivel de diseño, la **disposición de las opciones** y la **navegación fluida** fueron consideradas cruciales para facilitar una experiencia sin obstáculos ni confusión.

2. Seguridad y Protección

La **seguridad** fue un tema ampliamente tratado y muy valorado por los usuarios. Los participantes destacaron que la aplicación ofrece **una protección sólida** contra **ataques de Sim Swapping** y **Fake Apps**. Muchos comentarios señalaron que las **alertas de seguridad** fueron **claras** y **oportunas**, lo que ayudó a generar una sensación de **seguridad y confianza** durante las transacciones bancarias.

La implementación de **múltiples capas de seguridad**, como la **autenticación multifactorial**, fue especialmente destacada. Comentarios como “**la autenticación por huella es rápida y eficiente**” y “**la autenticación en tres pasos (IMEI, OTP y huella digital) me dio confianza total**” resaltan cómo estas características de seguridad mejoraron la protección sin complicar el proceso de acceso y uso de la aplicación.

Varios participantes también mencionaron que se sintieron **protegidos en cada transacción que realizaron**, lo que demuestra que la **seguridad multicapa** implementada en la aplicación fue efectiva para prevenir **accesos no autorizados** o **fraudulentos**. Los **intentos de acceso no autorizado** fueron bloqueados sin afectar la experiencia de usuario, y muchos se sintieron tranquilos al saber que la aplicación detectaba de manera eficiente cualquier **actividad sospechosa**. La implementación de **geolocalización** y **validación del IMEI** fue mencionada como una ventaja adicional que refuerza la seguridad.

Algunos encuestados también destacaron que la **protección contra fraudes** fue efectiva sin ser intrusiva, lo que sugiere que las medidas de seguridad no interfirieron significativamente con la experiencia de uso. Los participantes reconocieron que la **validación biométrica** y el **sistema OTP** funcionaron de manera

rápida y confiable, lo que contribuyó a una sensación de **protección** adicional durante las transacciones bancarias.

3. Interfaz y Diseño

En cuanto al **diseño de la interfaz**, los comentarios fueron en su mayoría positivos. Los participantes mencionaron que la **interfaz es limpia, moderna y sin distracciones**, lo que permite que los usuarios se concentren en las tareas sin sentirse sobrecargados de información. La **disposición de los menús** también fue destacada, ya que las opciones fueron fácilmente accesibles y la navegación fue clara y directa.

Algunos usuarios mencionaron que **el diseño de la aplicación facilita las operaciones** al ser **intuitivo**, lo que elimina cualquier posible confusión al usarla. Esto también permitió que la **experiencia de usuario** fuera fluida y sin complicaciones. Las **funciones de seguridad** fueron integradas de manera natural en el diseño de la aplicación, lo que permitió que no se percibiera como una barrera, sino como un **complemento necesario** para una navegación segura.

Además, los participantes indicaron que **el modelo de seguridad no afectó negativamente la usabilidad** de la aplicación, lo que significa que los usuarios pudieron disfrutar de una experiencia de uso **rápida y eficiente** sin sacrificar la protección. Esto resalta la **combinación ideal de seguridad y facilidad de uso**, que es uno de los mayores logros de la aplicación.

4. Confianza y Fiabilidad

La **confianza** fue un factor fundamental en la evaluación de la aplicación. Muchos participantes manifestaron que se sintieron **seguros y protegidos** al utilizarla para realizar transacciones bancarias. Comentarios como “**me sentí protegido en cada transacción**” y “**la aplicación es confiable y cumple con altos estándares de seguridad**” fueron recurrentes entre los encuestados.

La combinación de **seguridad en tiempo real y protección contra amenazas** fue bien recibida, ya que los usuarios se sintieron protegidos ante posibles fraudes. Sin

embargo, algunos participantes expresaron ligeras **dudas sobre la confiabilidad a largo plazo** de la aplicación, con comentarios como “**sí, pero no la veo confiable**”, lo que sugiere que, a pesar de la alta satisfacción, algunos usuarios querían ser cautelosos al evaluar la efectividad de las medidas de seguridad a futuro.

5. Términos Comunes Relacionados con el Modelo de Seguridad

Durante las respuestas, surgieron varios términos y conceptos clave relacionados con el modelo de seguridad implementado en la aplicación. Estos términos ayudan a comprender mejor cómo la aplicación garantiza tanto la **usabilidad** como la **seguridad**. Algunos de los términos más mencionados fueron:

- **Autenticación Multifactorial:** Un método de seguridad que requiere múltiples formas de verificación para garantizar que el usuario es quien dice ser. En este caso, la autenticación se realiza a través de **huella digital**, **IMEI** y **OTP** (contraseña de un solo uso).
- **OTP (One-Time Password):** Contraseña de un solo uso que se genera y se envía al usuario para validar una transacción o acceso.
- **IMEI (International Mobile Equipment Identity):** Un identificador único asignado a cada dispositivo móvil, utilizado para verificar la legitimidad del dispositivo.
- **Sim Swapping:** Un tipo de fraude donde los atacantes logran acceder a la línea telefónica de la víctima al cambiar la tarjeta SIM.
- **Fake Apps:** Aplicaciones falsas que intentan suplantar aplicaciones legítimas para robar información personal.
- **Geolocalización:** Uso de la ubicación del dispositivo para proporcionar una capa adicional de seguridad, validando si una transacción proviene de una ubicación esperada.
- **Autenticación Biométrica:** Uso de características físicas del usuario, como la huella digital, para garantizar la autenticidad del acceso.

- **Protección Multicapa:** Un enfoque de seguridad que utiliza múltiples métodos para proteger al usuario de amenazas, en este caso, combinando OTP, IMEI y huella digital.
- **Protección en Tiempo Real:** Sistema que detecta y bloquea accesos o actividades fraudulentas de manera inmediata.

Conclusión

Las opiniones del grupo experimental reflejan un alto nivel de satisfacción con la **usabilidad**, la **seguridad** y el **diseño** de la aplicación bancaria. Los participantes destacaron la **protección contra ataques de Sim Swapping y Fake Apps**, y se sintieron **seguros y protegidos** al realizar transacciones. La **autenticación multifactorial**, la **geolocalización** y el uso de **IMEI y OTP** fueron elementos clave en la percepción de seguridad.

El diseño de la aplicación fue considerado **moderno, intuitivo y eficiente**, sin comprometer la experiencia de usuario. Aunque algunos participantes expresaron dudas sobre la confiabilidad futura, la mayoría destacó que la aplicación es **confiable, rápida y fácil de usar**, lo que contribuye a su alta aceptación entre los usuarios.

En términos generales, la **combinación de seguridad y usabilidad** en esta aplicación ha sido percibida positivamente, lo que la convierte en una herramienta eficaz y confiable para proteger las transacciones bancarias y la información del usuario frente a amenazas externas.

Anexo 6: Artículo de Contribución de la Tesis

REVISTA PERUANA DE COMPUTACIÓN Y SISTEMAS 2024 6(2):3-13
<https://doi.org/10.15381/rpcs.v6i2.29031>

ISSN Online: 2617-2003
 FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
 UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

Artículo de Contribución

Modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android

Sectrabank Model for Mitigating the Computer fraud in electronic operations through Banking Applications on Android Device

Jhon Melendez^{1,a}, Luis Rivera^{2,b}, Jorge Mayhuasca^{3,c}, José Herrera^{3,d}, Paulo Calderón^{3,e}, Yordy Benites^{3,f}

¹ Postgraduate Program of FISI, National University of San Marcos, Perú

² Mathematical Science Lab, Universidade Estadual do Norte Fluminense, Brazil

³ Faculty of Systems Engineering and Informatics, National University of San Marcos, Perú

^a Autor de correspondencia: jhon.melendez@unmsm.edu.pe, ORCID:<https://orcid.org/0000-0003-3613-2569>

^b E-mail: rivera@uenf.br, ORCID:<https://orcid.org/0000-0002-5029-2561>

^c E-mail: jmayhuasca@unmsm.edu.pe, ORCID:<https://orcid.org/0000-0002-1693-2115>

^d E-mail: jherreraqu@unmsm.edu.pe, ORCID:<https://orcid.org/0000-0002-8207-9714>

^e E-mail: paulocesar.calderon@unmsm.edu.pe, ORCID:<https://orcid.org/0009-0006-1953-993X>

^f E-mail: yordy.benites@unmsm.edu.pe, ORCID:<https://orcid.org/0009-0009-1031-8542>

Resumen

El cibercrimen es un problema global que afecta a diferentes sectores, especialmente al sector financiero, donde los ciberdelincuentes explotan la falta de conciencia de seguridad de los usuarios para obtener información confidencial, utilizando técnicas como el phishing, smishing, vishing y finalmente apoderarse de la clave OTP para realizar operaciones fraudulentas. El objetivo de la investigación es desarrollar el modelo SectraBank, que incorpora medidas de seguridad como el uso del código IMEI, la huella dactilar y la geolocalización para mitigar los ataques de fraude informático, en las modalidades de SIM Swapping y Fake App utilizadas por los cibercriminales para apoderarse de la clave OTP. Para evaluar la efectividad del modelo, se realizaron simulaciones de ataques reales en teléfonos móviles de 50 usuarios, divididos en grupos de control y experimental. Los resultados demostraron que SectraBank mitigó el 98% de los ataques de SIM Swapping y el 88% de los ataques de Fake App. Además, el 98% de los participantes manifestaron su disposición a adoptar el modelo. Los resultados son cruciales para el sector bancario, el modelo propuesto ofrece una estrategia de seguridad robusta que podría reducir significativamente el fraude informático mejorando la seguridad y confianza en las aplicaciones de la banca móvil.

Palabras clave: Fake App, SIM Swapping, Cibercrimen, Fraude informático, Seguridad móvil, Autenticación

Abstract

Cybercrime is a global problem that affects various sectors, particularly the financial sector, where cybercriminals exploit users' lack of security awareness to obtain confidential information through techniques such as phishing, smishing, vishing, and ultimately seizing the OTP code to carry out fraudulent transactions. The objective of this research is to develop the SectraBank model, which incorporates security measures such as the use of the IMEI code, fingerprint authentication, and geolocation to mitigate cyber fraud attacks, specifically in the forms of SIM Swapping and Fake Apps used by cybercriminals to capture the OTP code. To evaluate the effectiveness of the model, simulations of real attacks were conducted on mobile phones of 50 users, divided into control and experimental groups. The results demonstrated that SectraBank mitigated 98% of SIM Swapping attacks and 88% of Fake App attacks. Additionally, 98% of participants expressed their willingness to adopt the model. These results are crucial for the banking sector, as the proposed model offers a robust security strategy that could significantly reduce cyber fraud, enhancing both security and trust in mobile banking applications.

Keywords: Fake App, SIM Swapping, Cybercrime, Computer fraud, Mobile security, Authentication

Recibido: 19-09-2024 - Aceptado: 05-12-2024 - Publicado: 30-12-2024

Citar como:

Melendez et al. (2024). Modelo Sectrabank para mitigar el fraude informático en operaciones electrónicas a través de aplicaciones bancarias en dispositivos Android, 6(2):3-13. <https://doi.org/10.15381/rpcs.v6i2.29031>

© Los autores. Este artículo es publicado por la Revista Peruana de Computación y Sistemas de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos. Este es un artículo de acceso abierto, distribuido bajo los términos de la licencia Creative Commons Atribución 4.0 Internacional (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.es>) que permite el uso, distribución y reproducción en cualquier medio, siempre que la obra original sea debidamente citada de su fuente original.

1. Introducción

El fraude informático ha experimentado un crecimiento exponencial, afectando a millones de usuarios en todo el mundo, con particular énfasis en los clientes de instituciones financieras [1]. Los ciberdelinquentes aprovechan la falta de conciencia y preparación en temas de seguridad por parte de usuarios e instituciones, lo que facilita la explotación de vulnerabilidades para obtener beneficios económicos ilícitos [2]. La sofisticación de los ataques ha avanzado considerablemente, adoptando métodos complejos que superan las medidas de seguridad tradicionales, lo cual convierte al cibercrimen en una amenaza global de magnitud creciente (Informe del FBI sobre Crímenes en Internet, 2023) [3].

El objetivo principal de los ataques cibernéticos es la obtención de ganancias ilícitas mediante la suplantación de identidades, tanto de instituciones financieras como de sus clientes [4]. Estos fraudes se desarrollan típicamente en tres etapas: la captura de información bancaria de su víctima, la apropiación de cuentas y la ejecución de transacciones financieras fraudulentas. En la primera fase, los atacantes emplean técnicas como el phishing (correo electrónico), smishing (mensajes de texto) y vishing (llamadas telefónicas) para engañar a las víctimas y obtener sus credenciales [5]. Una vez con la información en su poder, utilizan aplicaciones falsas (Fake App) o realizan el intercambio de tarjetas SIM (SIM Swapping), para apoderarse de la clave OTP (Token Digital) recibida por los usuarios en sus dispositivos móviles y ejecutar transacciones en nombre del usuario comprometido [6].

Si bien existen propuestas enfocadas en la detección de estos ataques, los esfuerzos en la mitigación de sus efectos son limitados [7]. Los medios de comunicación informan constantemente sobre los daños causados por estos fraudes en servicios móviles, con pérdidas de miles de millones de dólares, cifras que demuestran la falta de suficientes técnicas actuales de mitigación [8]. La literatura señala que estas deficiencias pueden deberse a la insuficiente verificación en tiempo real de la identidad del usuario durante las transacciones electrónicas, especialmente en operaciones móviles (M-Oper) [9-10].

Además, investigaciones recientes han resaltado la importancia de combinar técnicas tradicionales con métodos innovadores para enfrentar la evolución constante de las amenazas [11]. Por ejemplo, se han propuesto nuevas metodologías para mejorar la autenticación multifactorial y la detección de fraudes [12]. A pesar de estos avances, el desafío persiste debido a la rápida adaptación de los atacantes a las medidas de seguridad existentes [13].

El uso de inteligencia artificial y aprendizaje automático también está siendo explorado para anticipar y prevenir ataques de manera más eficaz [14]. Sin embargo, la implementación de estas tecnologías aún enfrenta obstáculos significativos, como la necesidad de

grandes volúmenes de datos y la posibilidad de falsos positivos [15].

En este contexto, el presente estudio propone el modelo SectraBank, diseñado específicamente para mitigar ataques de SIM Swapping y aplicaciones falsas. SectraBank integra medidas de seguridad como el uso del código IMEI, la huella dactilar y la geolocalización del dispositivo, brindando una protección robusta a lo largo de todas las fases de la transacción. El objetivo del modelo es mejorar la seguridad y aumentar la confianza en las operaciones de banca móvil, demostrando que un enfoque basado en múltiples capas de seguridad puede reducir considerablemente la vulnerabilidad ante ataques cibernéticos.

2. Ciber Ataques

Los ciberataques y el fraude informático aumentan significativamente cada año, afectando a las instituciones financieras y sus clientes. El FBI reportó un incremento del 300% en pérdidas económicas debido a cibercrimen en los últimos cinco años, afectando tanto la seguridad financiera como la privacidad de los usuarios (Fig.1). En Perú, la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) informó un aumento del 200% en los ciberataques desde 2019, resaltando la creciente necesidad de reforzar las medidas de seguridad (Fig.2).

Figura 1

Efectos de los Ataques Cibernéticos: A Nivel Mundial (Informes de Crímenes en Internet del FBI 2023)

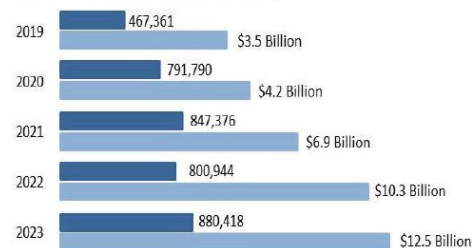


Figura 2

Efectos de los Ataques Cibernéticos: DIVINDAT-Perú (2023)



En respuesta, investigaciones recientes han recurrido a técnicas de inteligencia artificial (IA) para mejorar la ciberseguridad. No obstante, los ciberdelincuentes también emplean IA para llevar a cabo ataques cada vez más sofisticados. Estos incluyen la suplantación de identidad mediante técnicas como el Phishing, Smishing y Vishing [12-15].

Generalmente, los ciberdelincuentes se hacen pasar por funcionarios y clientes de instituciones financieras para apoderarse de recursos valiosos, como se ilustra en la Fig. 3. Una de las principales vías para estos ataques son las transacciones realizadas mediante dispositivos móviles, lo que aumenta la vulnerabilidad de los clientes que operan en plataformas de banca digital, convirtiéndolos en un objetivo prioritario para los ciberdelincuentes.

En muchos casos, los ciberdelincuentes logran apropiarse de información confidencial, como números de cuenta, claves y números de teléfono, utilizando estas técnicas, las cuales son las más reportadas según DIVINDAT (Fig. 4).

Entre las estrategias de defensa, destacan los modelos de aprendizaje automático y profundo. Modelos como el propuesto por Aljofey et al. [16],

que usa redes neuronales convolucionales (CNN) para detectar Phishing, y otros enfoques híbridos como el de Shaiba et al. [4] y Roy et al. [17] han alcanzado precisiones de hasta el 99%. En el análisis de URLs de phishing, técnicas como las redes neuronales recurrentes (RNN) y la memoria a largo plazo (LSTM) también han mostrado una alta efectividad, superando el 98% de precisión en múltiples estudios [18-20].

El Smishing, que combina Phishing y SMS, ha sido abordado por autores como Mishra & Soni [14], quienes lograron un 96% de precisión en la detección de mensajes fraudulentos mediante análisis del comportamiento de URLs y APKs maliciosos. En el caso del Vishing, técnicas como las redes CNN y BiLSTM han mostrado gran eficacia en la detección de fraude en voz [21]. Para otros ataques como el SIM Swapping y el uso de aplicaciones falsas (Fake Apps), estudios de Tang et al. [22] y Gezer et al. [23] revelan cómo los ciberdelincuentes logran interceptar códigos de autenticación OTP y tomar control de las cuentas bancarias de las víctimas.

Finalmente, se ha identificado la necesidad de más investigaciones en técnicas de mitigación, especialmente para el SIM Swapping y las aplicaciones falsas. Algunas propuestas incluyen el uso de modelos híbridos como el de Prayogi & Aji [24], que combina infraestructuras móviles con algoritmos de inteligencia artificial para detectar anomalías en tiempo real, logrando una efectividad superior al 99%.

3. Modelo SectraBank

El modelo propuesto ha sido diseñado e implementado con el fin de mitigar ataques de fraude informático en las modalidades de SIM Swapping y aplicaciones falsas (Fake Apps). Para su desarrollo, se ha llevado a cabo una investigación exhaustiva sobre el comportamiento cibercriminal del atacante, estableciendo tres fases críticas, como se muestra en la Fig. 5.

Figura 3

Ataques cibernéticos usuales

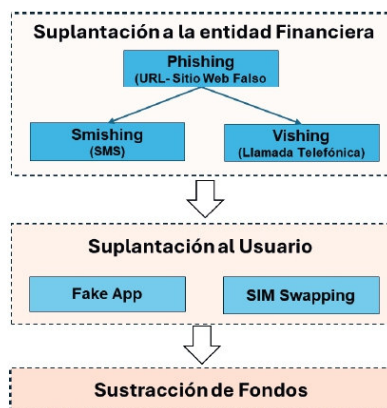


Figura 4

Segmentación de Ataques por Modalidad (DIVINDAT-Perú, 2023)

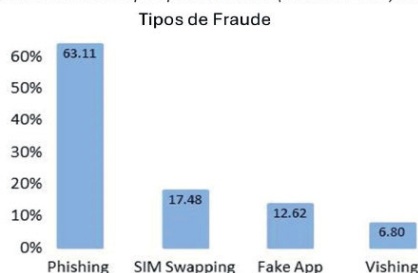
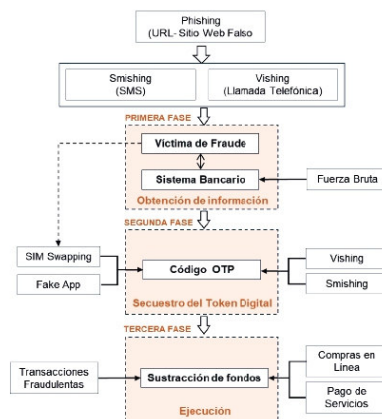


Figura 5

Estructura del proceso de fraude



En la primera fase, el cibercriminal accede a información sensible de la víctima, como los datos de su tarjeta bancaria y el número de teléfono asociado a sus cuentas. Esta información puede ser obtenida mediante técnicas de ingeniería social como el phishing y sus variantes, o, en algunos casos, mediante ataques de fuerza bruta.

Durante la segunda fase, el atacante emplea métodos de intercambio de SIM y la creación o distribución de aplicaciones maliciosas (Fake Apps) para interceptar el código de verificación de un solo uso (OTP) enviado al dispositivo móvil de la víctima. Esta etapa es crucial, ya que permite al atacante superar los mecanismos de autenticación de dos factores implementados por las instituciones financieras.

En la tercera fase, el atacante utiliza la información obtenida y el acceso a la cuenta de la víctima para realizar transacciones fraudulentas. Estas acciones pueden incluir transferencias bancarias no autorizadas, compras en línea o el pago ilícito de servicios. El modelo SectraBank está diseñado específicamente para interrumpir este ciclo, previniendo la materialización de dichas actividades fraudulentas.

3.1. Medidas de seguridad implementadas por el modelo Sectrabank

El modelo SectraBank propuesto, utiliza como medida de seguridad para mitigar los ataques de Fake App y SIM Swapping, el IMEI del dispositivo, la geolocalización y la huella dactilar, con lo cual se impedirá el secuestro y obtención del código OTP o clave dinámica, generada aleatoriamente por el sistema del banco. El modelo cuenta con tres capas de seguridad. La primera capa, la externa, consiste en la validación de la contraseña. La segunda capa, la intermedia, requiere la verificación mediante un atributo biométrico del usuario. Y la tercera capa, la interna, verifica la geolocalización del solicitante de la operación, conforme se detalla a continuación.

- a. **Primera capa de seguridad:** Esta fase implica validar las credenciales bancarias con el código IMEI (CI) del dispositivo telefónico del cliente. En esta etapa, SectraBank mitigará el ataque de

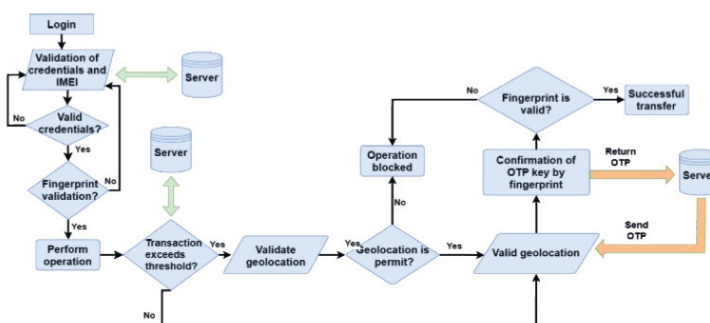
SIM Swapping después de que el atacante tome el control de la línea telefónica y/o tarjeta SIM de la víctima e intente insertarla en otro dispositivo telefónico para acceder a la clave dinámica o contraseña OTP. La aplicación con los datos bancarios será bloqueada debido a la validación incorrecta del IMEI con los datos bancarios.

- b. **Segunda capa de seguridad:** La verificación en este nivel ocurre cuando el supuesto cliente ha pasado exitosamente la validación OTP. En esta etapa, el solicitante debe confirmar con su atributo biométrico, como una huella dactilar. Si el usuario no cumple con este proceso de validación, la operación será bloqueada. Esta medida fortalece significativamente la integridad del modelo SectraBank, proporcionando una capa adicional de protección contra posibles intentos de acceso remoto no autorizado, mitigando así los ataques de Fake App.
- c. **Tercera capa de seguridad:** La efectividad de esta capa de seguridad se basa en la geolocalización y el establecimiento de un umbral máximo de transferencia. Este umbral puede ser definido por el usuario y ajustado a través de un análisis de sus patrones históricos de comportamiento bancario. Para los nuevos usuarios, se establece un umbral predeterminado en coordinación con el banco. Para realizar transferencias que excedan el umbral establecido por el usuario y el banco, o para transacciones de alto valor, es necesario estar en una ubicación preestablecida designada como zona segura, delimitada por una geomalla. Las dos primeras capas de seguridad están diseñadas para reducir el riesgo de fraude informático, especialmente en las modalidades de Fake Apps y SIM swapping. En caso de que estas medidas de seguridad sean eludidas, se activará la tercera capa de seguridad, proporcionando una protección adicional.

3.2. Proceso de las Capas de Seguridad

La Fig. 6 muestra el flujo de acción de las capas de seguridad del modelo SectraBank. En la primera capa de

Figura 6
Proceso de Capa de Seguridad



seguridad, se validan las credenciales del usuario, como el número de cuenta, la contraseña y el código IMEI el cual es comparada con la información almacenada en el servidor de la institución financiera. La segunda capa de seguridad involucra la validación de la huella dactilar del usuario. Si esta no es validada, se solicita nuevamente las credenciales, y en el tercer intento fallido, se bloquea la aplicación. Con estas dos capas, SectraBank mitiga los ataques de Fake App y SIM Swapping.

Como medida adicional, se implementa una tercera capa de seguridad basada en la geolocalización. El usuario puede designar tres sectores frecuentes para realizar transacciones que excedan un umbral de saldo acordado con el banco. Es necesario estar en una de las zonas seguras designadas para realizar estas transacciones, delimitadas por una geomalla. Si el usuario no se encuentra en la zona segura, la transacción se cancela. La validación de la clave OTP se realiza a través de la verificación de la huella dactilar.

3.3. Código Fuente utilizado en el desarrollo del modelo

El modelo SectraBank fue desarrollado en Java con Spring Boot para el backend y Kotlin para el frontend, utilizando MySQL como base de datos. El sistema incorpora medidas de seguridad avanzadas para mitigar ataques de fraude, como Fake App y SIM Swapping, en transacciones electrónicas. La aplicación requiere permisos como acceso a la ubicación (FusedLocationProviderClient), estado del teléfono (READ_PHONE_STATE) y autenticación por huella digital (USE_FINGERPRINT). Además, implementa autenticación biométrica mediante huella, recuperación del IMEI del dispositivo para garantizar seguridad, y generación de códigos OTP para autorizar transacciones. Todas estas medidas fortalecen la protección del usuario y garantizan el cumplimiento de normativas de privacidad y seguridad. Una explicación más detallada del código fuente se encuentra en el Apéndice 2.

3.4. Diseño del Modelo

El diseño del modelo SectraBank implementado para la plataforma Android, presenta cuatro interfaces, como se muestra en la Fig. 7, que son: Interfaz de Inicio de Sesión y Panel Principal.

En la Fig. 8 Se muestra el diseño de la primera, segunda y tercera capa de seguridad. En la primera capa, la sesión se inicia únicamente mediante la validación de credenciales correctas, como el IMEI registrado y la huella dactilar, como se ilustra en la Fig. 8 (a). Si el IMEI, la contraseña o la huella dactilar son incorrectos, no se permitirá el inicio de sesión, mostrando un mensaje de error en la verificación del usuario. Esto mitiga el ataque de SIM Swapping. La Fig. 8 (b) muestran el funcionamiento de la tercera capa de seguridad, que

permite al usuario elegir tres puntos de ubicación para validar transacciones que excedan un cierto umbral del saldo total de la cuenta, establecido en coordinación con el banco. Este proceso se implementa como una medida de seguridad adicional contra transferencias desde ubicaciones geográficas no autorizadas.

Si se detecta una solicitud de transferencia desde una geolocalización fuera de la geomalla establecida, la transacción será inválida, con lo cual se mitigará los ataques de fraude informático en la modalidad de Fake App.

Cuando el usuario ingresa el número de cuenta bancaria y el monto de la transacción, para completar la operación, el sistema genera un token o clave dinámica que se envía a través de un mensaje OTP por SMS

Figura 7
Interfaz de Inicio de Sesión (a) y Panel de control (b)

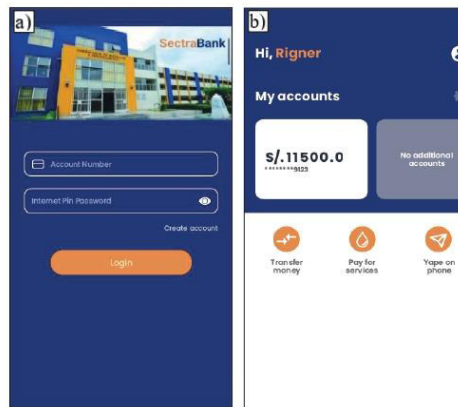


Figura 8
Autenticación de Huella dactilar para ingreso y selección de puntos en el mapa

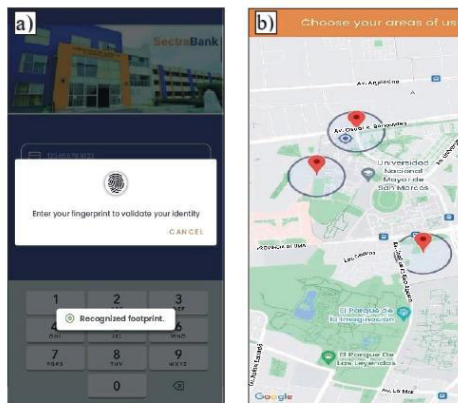
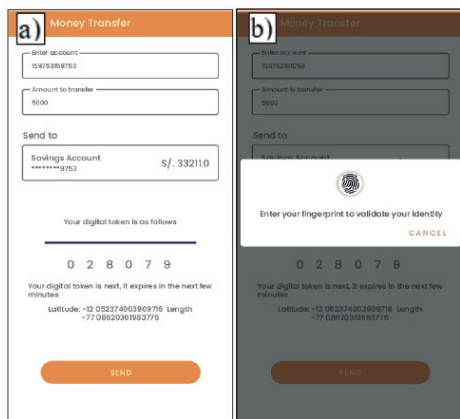


Figura 9
Mensaje OTP (a) y Validación de Huella dactilar (b)



al teléfono móvil, como se ilustra en la Fig. 9(a). La confirmación final necesariamente se realiza con la validación de huella dactilar, como se muestra en la Fig. 9(b). Finalmente, el proceso concluye con la emisión de un mensaje de confirmación de la transferencia.

4. Metodología y Evaluación

La metodología empleada para la evaluación del modelo SectraBank sigue un enfoque de investigación aplicada con un diseño experimental. Se conformaron dos grupos: uno de control y otro experimental, cada uno compuesto por 25 participantes, lo que hace un total de 50 usuarios. El diseño permitió comparar el impacto del modelo SectraBank en la mitigación de ataques de SIM Swapping y Fake App, evaluando los resultados entre ambos grupos bajo condiciones controladas. El grupo de control utiliza la aplicación bancaria estándar, sin las medidas de seguridad adicionales. El grupo experimental emplea el modelo SectraBank con la implementación de las tres capas de seguridad. Los participantes son seleccionados al azar, y las variables clave incluyen la incidencia de ataques y la efectividad de las contramedidas implementadas. El objetivo es determinar la mitigación de los ataques de fraude informático en la modalidad de SIM Swapping y Fake App.

4.1. Selección de los participantes

Se seleccionaron 50 participantes, compuestos por estudiantes de Ingeniería de Software de la Universidad Nacional de San Marcos y personal policial de la DIVINDAT, encargados de investigar delitos informáticos. El requisito principal fue el uso de teléfonos con sistema operativo Android. Los policías, con conocimiento especializado en modalidades de fraude cibernético como Fake App y SIM Swapping, actuaron en lugar de expertos en ciberseguridad.

De los 50 participantes, 25 formaron el grupo de control, instalando la aplicación SectraBank sin medidas de seguridad adicionales. Los otros 25 conformaron el grupo experimental, utilizando la aplicación con las medidas de seguridad implementadas: código IMEI, huella dactilar y geolocalización.

4.2. El Experimento

El experimento se realiza en tres fases: configuración inicial, implementación del modelo y simulación de ataques.

4.2.1. Fase 1: Configuración Inicial

Se buscó asegurar que los grupos de control y experimental tuvieran perfiles similares en términos de demografía y uso de tecnología, considerando edad, género, nivel educativo, ocupación y uso de tecnología. Los criterios de selección fueron:

- Edades entre 26 y 40 años.
- Igual cantidad de hombres y mujeres en cada grupo.
- Igual número de estudiantes y policías expertos en delitos cibernéticos.
- Uso similar de tecnología en cuanto a aplicaciones y frecuencia.

Ambos grupos recibieron una introducción sobre el funcionamiento de SectraBank y sobre los ataques cibernéticos, como Fake App y SIM Swapping.

4.2.2. Fase 2: Implementación del Modelo

Grupo de Control: Se les proporcionó el modelo SectraBank sin las medidas de seguridad adicionales.

Grupo Experimental: Se les proporcionó la aplicación bancaria con el modelo SectraBank implementado, incluyendo las medidas de seguridad del código IMEI, huella dactilar y geolocalización.

4.2.3. Fase 3: Simulación de Ataques

Fake App: Se informó a los participantes sobre la importancia de las medidas de seguridad y las técnicas de ataque Fake App. Con su consentimiento, se simuló un ataque que permitía acceso remoto a sus teléfonos para realizar transferencias bancarias simuladas.

SIM Swapping: Se explicó el ataque SIM Swapping y, con consentimiento, se simuló este ataque para realizar transferencias desde los teléfonos de los participantes.

Los resultados se recopilaban para determinar cuántos usuarios de ambos grupos fueron comprometidos.

4.3. Medición y Análisis de Resultados

La información generada en el experimento y las respuestas de los 50 participantes son analizadas.

Tabla 1

Resultados empíricos de la simulación de ataques

Intentos de ataque	SIM Swapping		Fake App	
	Control	Experimental	Control	Experimental
Ataques exitosos	20	2	22	3
Ataques bloqueados	5	23	3	22
Éxitos (%)	80%	8%	88%	12%
Bloqueos (%)	20%	92%	12%	88%

Recopilación de Datos: En la simulación de ataques de SIM Swapping y Fake App, los 50 usuarios se agrupan en los grupos de control y experimental, como se registra en la Tabla 1. Las columnas respectivas indican los intentos de ataque que lograron vulnerar las capas y aquellos que no lograron vulnerar las capas.

Las figuras 10 y 11 ilustran los casos exitosos de mitigación de ataques de intercambio de SIM y aplicaciones falsas y la baja tasa de éxito de los ataques.

Para SIM Swapping, la tasa de éxito de los ataques en el grupo de control fue del 12%, mientras que en el grupo experimental fue del 92%. Esto indica que las medidas de seguridad implementadas fueron muy efectivas para reducir la tasa de éxito de los ataques.

Figura 10

Gráfica de los resultados de SIM Swapping

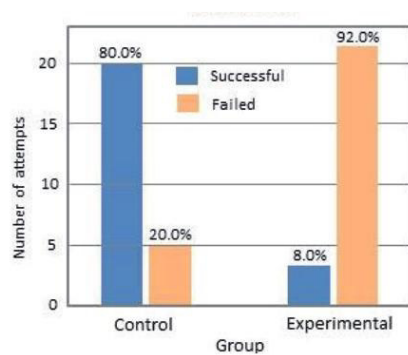
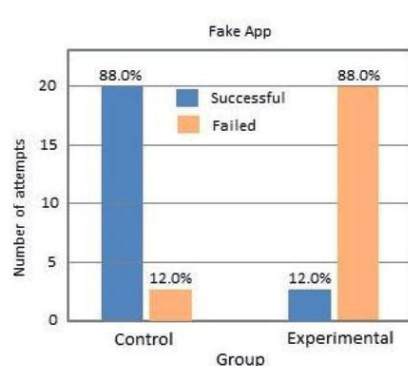


Figura 11

Gráfica de los resultados de Fake app



Para Fake App, la tasa de éxito de los ataques en el grupo de control fue del 88%, mientras que en el grupo experimental fue del 12%. Esto muestra que las medidas de seguridad implementadas fueron altamente efectivas para mitigar los ataques de Fake App.

Las medidas de seguridad implementadas en el modelo SectraBank han demostrado ser muy efectivas en la mitigación de ataques de SIM Swapping y Fake App, reduciendo significativamente la tasa de éxito de los intentos de acceso no autorizado en el grupo experimental en comparación con el grupo de control.

Encuestas de Satisfacción

Según el análisis de los datos recopilados, se encontró que el 98% de los participantes usarían el modelo propuesto. Este resultado refleja una alta aceptación y confianza en las medidas de seguridad de este método para acceder a sus cuentas a través de la tecnología móvil.

4.4. Validación Estadística de la Mitigación de Ataques de SIM Swapping y Fake App: Resultados Empíricos

4.4.1. Para el grupo de control:

A los usuarios se les proporcionó el modelo SectraBank sin las medidas de seguridad adicionales.

a. SIM Swapping: En el grupo de control, 20 de los ataques de SIM Swapping fueron exitosos, lo que significa que los atacantes lograron vulnerar las medidas de seguridad estándar 20 veces. Solo 5 ataques fueron bloqueados, indicando que las medidas de seguridad estándar no fueron muy efectivas.

b. Fake App: En el grupo de control, 22 ataques de Fake App fueron exitosos, y solo 3 fueron bloqueados, sugiriendo que las medidas de seguridad estándar tampoco fueron muy efectivas contra este tipo de ataque.

4.4.2. Para el grupo experimental:

A los usuarios, se les proporcionó la aplicación bancaria con el modelo SectraBank implementado, incluyendo las medidas de seguridad del código IMEI, huella dactilar y geolocalización. Obteniendo el siguiente resultado:

a. SIM Swapping: En el grupo experimental, solo 2 ataques de SIM Swapping fueron exitosos, mientras que 23 ataques fueron bloqueados. Esto indica que las nuevas medidas de seguridad fueron

Tabla 2

Resultados de la Prueba Z para Comparación de Proporciones en Fraudes de SIM Swapping y Fake App

Caso	Grupo	Proporción ($\hat{p}$)	Estadístico Z	Valor p
SIM Swapping	Control	0.8	5.13	$\approx 2.90 \times 10^{-7}$
	Experimental	0.08		
Fake App	Control	0.88	5.37	$\approx 7.87 \times 10^{-8}$
	Experimental	0.12		

mucho más efectivas que las del grupo de control, ya que bloquearon una mayor cantidad de ataques.

- b. Fake App: En el grupo experimental, 3 ataques de Fake App fueron exitosos, mientras que 22 fueron bloqueados. Similarmente, esto muestra que las nuevas medidas de seguridad implementadas en el grupo experimental fueron significativamente más efectivas que las del grupo de control.

4.4.3. Resultados estadísticos del modelo Sectrabank

El modelo Sectrabank ha demostrado ser altamente efectivo en la mitigación de ataques tanto para SIM Swapping como para Fake App. Los resultados muestran un incremento significativo en la proporción de ataques bloqueados en el grupo experimental comparado con el grupo de control, lográndose mitigar el 92% de ataques de SIM Swapping y 88% de ataques de Fake App, demostrando con ello la efectividad en la mitigación de ataques de estudiados, en la Tabla 2 se puede observar el análisis estadístico realizado y el valor Z que indica que hay una diferencias significativa amplia con respecto de la aplicación y no aplicación del modelo propuesto.

5. Conclusiones

Las técnicas de ciber ataques, como el uso de aplicaciones falsas (Fake App) y el intercambio de tarjetas SIM (SIM Swapping), representan amenazas significativas para la seguridad financiera en el ámbito digital. Tras llevar a cabo exhaustivas simulaciones de ataques en dispositivos móviles reales, el modelo SectraBank ha demostrado ser una solución altamente eficaz y viable para mitigar estas modalidades de fraudes, con tasas de efectividad del 92% en la detección de SIM Swapping y del 88% en la identificación de aplicaciones falsas, junto con una aceptación del 98% por parte de los usuarios, los resultados obtenidos resaltan la importancia de implementar estrategias de seguridad robustas e integradas como el modelo SectraBank que combina tecnologías avanzadas como el código IMEI, la autenticación biométrica mediante huella digital y la geolocalización, estableciendo un estándar en la prevención de fraudes informáticos. Este enfoque integral ha demostrado ser crucial para fortalecer la protección contra el fraude informático en las modalidades de Fake App y SIM Swapping, bloqueando de manera efectiva el acceso no autorizado al código OTP (token de un solo uso).

Es imperativo considerar que el modelo propuesto está diseñado con limitaciones de desarrollo que lo restringen exclusivamente a dispositivos móviles que

funcionan con el sistema operativo Android, con excepción de los teléfonos HUAWEI. Esta restricción surge de las sanciones impuestas por Google al fabricante HUAWEI, impactando en la compatibilidad del modelo con estos dispositivos.

6. Referencias

- [1] Tabassum, N., Neha, F., Hossain, M., et al. (2021) 'A hybrid machine learning based phishing website detection technique through dimensionality reduction', IEEE Int. Black Sea Conf. Commun. Networking, pp. 1-6. <https://doi.org/10.1109/BlackSeaCom52164.2021.9527806>
- [2] Sahingoz, O.K., Buber, E., et al. (2019) 'Machine learning-based phishing detection from URLs', Expert Syst. Appl., 117, pp. 345-357. <https://doi.org/10.1016/j.eswa.2018.09.029>
- [3] Kim, M., Suh, J., Kwon, H. (2022) 'A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures', IEEE/ACIS 7th Int. Conf. Big Data, Cloud Comput., Data Sci. (BCD), pp. 240-245. <https://doi.org/10.1109/BCD54882.2022.9900510>
- [4] Shaiba, H., Alzahrani, J., Eltahir, M., et al. (2022) 'Hunger Search Optimization with Hybrid Deep Learning Enabled Phishing Detection and Classification Model', Comput. Mater. Continua, 73(3), pp. 6425-6441. DOI: 10.32604/cmc.2022.031625
- [5] Feizi-Derakhshi, M., Zafarani-Moattar, E., Ala'a Al-Kabi, H., et al. (2024) 'Pcf: Parallel cnn-lstm fusion model for sms spam filtering', BIO Web Conf., p. 136. <https://doi.org/10.1051/bioconf/20249700136>
- [6] Jain, A., Gupta, B., Kaur, K., et al. (2022) 'A content and URL analysis-based efficient approach to detect smishing SMS in intelligent systems', Int. J. Intell. Syst., 37(12), pp. 11117-11141. <https://doi.org/10.1002/int.23035>
- [7] Kumar, D., Hemanth, N., Premnath, S., et al. (2020) 'Detection of phishing websites using an efficient machine learning framework', Int. J. Eng. Res. Technol., 9(5), pp. 1282-1286. <https://d1wqtxts1xzle7.cloudfront.net/63544102/detection-of-phishing-websites-using>
- [8] Carvalho, S., Carvalho, J., Silva, J., et al. (2023) 'Concerns about Cybersecurity: The Implications of the use of ICT for Citizens and Companies', J. Inf. Syst. Eng. Manag., 8(2). <http://dx.doi.org/10.55267/iadt.07.13226>
- [9] Darem, A., Alhashmi, A., Alkhaldi, T., et al. (2023) 'Cyber threats classifications and countermeasures in banking and financial sector', IEEE Access, pp. 125138-125158. <https://doi.org/10.1109/ACCESS.2023.3327016>
- [10] Ren, Y., Wang, C., Chen, Y., et al. (2019) 'Signature verification using critical segments for securing mobile transactions', IEEE Trans. Mob. Comput., 19(3), pp. 724-739. <https://doi.org/10.1109/TMC.2019.2897657>

- [11] Sharma, G., Ghosh, M. (2021) 'A Secure Lightweight Authentication Protocol for Mobile Payment', pp. 515-527. https://doi.org/10.1007/978-981-15-9774-9_48
- [12] Kuttiyappan, D., Rajasekar, V. (2023) 'Improving the Cyber Security over Banking Sector by Detecting the Malicious Attacks Using the Wrapper Stepwise Resnet Classifier', KSII Trans. Internet Inf. Syst., 17(6), pp. 1657-1673. <https://doi.org/10.3837/tiis.2023.06.007>
- [13] Panda, P., Mishra, A., Puthal, D. (2022) 'A novel logo identification technique for logo-based phishing detection in cyber-physical systems', Future Internet, 14(8), p. 241. <https://doi.org/10.3390/fi14080241>
- [14] Mishra, S., Soni, D. (2020) 'Smishing detector: A security model to detect smishing through sms content analysis and url behavior analysis', Future Gen. Comput. Syst., 108, pp. 803-815. <https://doi.org/10.1016/j.future.2020.03.021>
- [15] Armstrong, M., Jones, K., Namin, A. (2021) 'How perceptions of caller honesty vary during vishing attacks that include highly sensitive or seemingly innocuous requests', Hum. Factors, 65(2), pp. 275-287. <https://doi.org/10.1177/00187208211012818>
- [16] Aljofey, A., Jiang, Q., Qu, Q., et al. (2020) 'An effective phishing detection model based on character level convolutional neural network from url', Electronics, 9(9). <https://doi.org/10.3390/electronics9091514>
- [17] Roy, S., Awad, A., Amare, L., et al. (2022) 'Multimodal phishing url detection using lstm, bidirectional lstm, and gru model', Future Internet, 14(11), p. 340. <https://doi.org/10.3390/fi14110340>
- [18] Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., et al. (2023) 'A deep learning-based phishing detection system using cnn, lstm, and lstm-cnn', Electronics, 12(1), p. 232. <https://doi.org/10.3390/electronics12010232>
- [19] Elsadig, M., Ibrahim, A., Basheer, S., et al. (2022) 'Intelligent deep machine learning cyber phishing url detection based on bert features extraction', Electronics, 11(22), p. 3647. <https://doi.org/10.3390/electronics11223647>
- [20] Alqahtani, H., Alotaibi, S., Alrayes, F., et al. (2022) 'Evolutionary Algorithm with Deep Auto Encoder Network Based Website Phishing Detection and Classification', Appl. Sci., 12(15), p. 7441. <https://doi.org/10.3390/app12157441>
- [21] Moussavou Boussougou, M., Park, D. (2023) 'Attention-based 1d cnn-bilstm hybrid model enhanced with fasttext word embedding for korean voice phishing detection', Mathematics, 11(14), p. 3217. <https://doi.org/10.3390/math11143217>
- [22] Tang, C., Chen, S., Fan, L., et al. (2019) 'A large-scale empirical study on industrial fake apps', In 2019 IEEE/ACM 41st Int. Conf. Softw. Eng.: Softw. Eng. Pract. (ICSE-SEIP), pp. 183-192. <https://doi.org/10.1109/ICSE-SEIP.2019.00028>
- [23] Gezer, A., Warner, G., Wilson, C., et al. (2019) 'A flow-based approach for trickbot banking trojan detection', Comput. Secur., 84, pp. 179-192. <https://doi.org/10.1016/j.cose.2019.03.013>
- [24] Prayogi, A., Aji, R. (2023) 'Utilization of mobile network infrastructure to prevent financial mobile application account takeover', Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 7(4), pp. 797-808. <https://doi.org/10.29207/resti.v7i4.50254>

Anexo 7 : Actas de validación de herramientas de recopilación de datos

1) Dr. Cayo Victor León Fernandez



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

DOCTORADO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TÍTULO DE TESIS: "Modelo Sectrabank para Mitigar el Fraude Informático en Operaciones Electrónicas a través de Aplicaciones Bancarias en Dispositivos Android"

AUTOR: Jhon Rigner MELENDEZ MELENDEZ

ASESOR: Dr. Jorge Victor MAYHUASCA GUERRA

APELLIDOS Y NOMBRES DEL JUEZ:	CAYO VICTOR LEON FERNANDEZ
DNI:	07001405
FORMACIÓN ACADÉMICA:	DOCTOR EN INGENIERÍA INFORMÁTICA Y SISTEMAS
ÁREA DE EXPERIENCIA PROFESIONAL:	DOCENTE
INSTITUCIÓN:	UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

Firma del experto informante



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

RESUMEN

El cibercrimen es un problema global que afecta a diferentes sectores, especialmente al sector financiero, donde los ciberdelincuentes explotan la falta de conciencia de seguridad de los usuarios para obtener información confidencial, utilizando técnicas como el phishing, smishing, vishing y finalmente apoderarse de la clave OTP para realizar operaciones fraudulentas. El objetivo de la investigación es desarrollar el modelo SectraBank, que incorpora medidas de seguridad como el uso del código IMEI, la huella dactilar y la geolocalización para mitigar los ataques de fraude informático, en las modalidades de SIM Swapping y Fake App utilizadas por los cibercriminales para apoderarse de la clave OTP. Para evaluar la efectividad del modelo, se realizaron simulaciones de ataques reales en teléfonos móviles de 50 usuarios, divididos en grupos de control y experimental. Los resultados demostraron que SectraBank mitigó el 98% de los ataques de SIM Swapping y el 88% de los ataques de Fake App. Además, el 98% de los participantes manifestaron su disposición a adoptar el modelo. Los resultados son fundamentales para el sector bancario, ya que el modelo propuesto brinda una estrategia de seguridad integral que puede reducir de manera significativa el fraude informático, reforzando la protección y la confianza en las aplicaciones de banca móvil.

Palabras clave: Fake App, SIM Swapping, Cibercrimen, Fraude informático, Seguridad móvil, Autenticación.

Firma del experto informante

Instrucciones:

Coloque en cada casilla un aspa correspondiente al aspecto cualitativo de cada ítem y alternativa de respuesta.

Las categorías a evaluar son: Redacción, contenido, con los indicadores, dimensiones y variables de estudio. En la casilla de observaciones puede sugerir el cambio o mejora de cada pregunta.



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: V1 MARCO DE TRABAJO

N.º	DIMENSIONES / INDICADORES	ÍTEMS/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
			SI	NO	SI	NO	SI	NO	
	DIMENSIÓN 1: Conocimiento y experiencia sobre fraude informático y su entorno		SI	NO	SI	NO	SI	NO	
1	Conocimiento de las operaciones bancarias	¿Usted realiza operaciones bancarias?	X		X		X		
2	Conocimiento de ataques específicos de fraude informático	¿Tienes conocimiento de los ataques de fraude informático en la modalidad de Fake App y SIM Swapping?	X		X		X		
3	Experiencia personal con el fraude informático	¿Usted, su entorno amical o familiar, ¿En alguna oportunidad ha sido víctima de fraude informático?	X		X		X		
4	Conciencia y experiencia previa en el reconocimiento de intentos de fraude informático mediante técnicas de ingeniería social.	¿Ha recibido mensajes sospechosos relacionados con operaciones bancarias (phishing, smishing)?	X		X		X		
5	Nivel de conocimiento sobre herramientas tecnológicas avanzadas aplicadas a la seguridad bancaria.	¿Está familiarizado con el término "geolocalización" para la seguridad bancaria?	X		X		X		
6	Interés en fortalecer sus habilidades y conocimientos sobre prevención de fraudes.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
7	Intención de adopción de tecnologías específicas para la protección contra fraudes informáticos.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X			X	
	DIMENSIÓN 2: Usabilidad y percepción de aplicaciones bancarias con el modelo propuesto		SI	NO	SI	NO	SI	NO	
8	Percepción del usuario respecto al UX del modelo sectrabank	¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular?		X		X	X		
9	Percepción de confianza en la seguridad de las transacciones	¿Qué tan seguro se siente al realizar transferencias de gran monto por aplicaciones móviles?	X		X		X		



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

N.º	DIMENSIONES / INDICADORES	ÍTEMS/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
	electrónicas realizadas mediante aplicaciones móviles.								
10	Conocimiento de buenas prácticas en la instalación y uso seguro de aplicaciones móviles.	¿Pienso que la instalación de aplicaciones desde fuentes oficiales reduce el riesgo de fraude?		X		X	X		
	DIMENSION 3: Evaluación del modelo propuesto		SI	NO	SI	NO	SI	NO	
11	Evaluación sobre la eficacia del modelo en casos de Fake App	¿Considera que el modelo propuesto ha mitigado el ataque simulado de Fake App ejecutado en su dispositivo móvil?	X		X		X		
12	Evaluación sobre la eficacia del modelo en casos de SIM Swapping	¿Considera que el modelo propuesto ha mitigado el ataque simulado de SIM Swapping ejecutado en su dispositivo móvil?	X		X		X		
13	Disposición para usar la aplicación	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?		X	X		X		
14	Percepción de impacto del modelo en la eficiencia operativa de las transacciones bancarias.	¿Considera que el modelo propuesto afecta la velocidad de las transacciones?	X		X		X		
15	Opinión del usuario sobre la eficacia de las medidas de seguridad basadas en autenticación biométrica y características del dispositivo.	¿Es suficiente el uso del IMEI y huella dactilar para proteger las operaciones bancarias?	X		X		X		
16	Disposición de los usuarios para adoptar soluciones tecnológicas que incorporen el modelo de mitigación de fraudes.	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?							

Muchas gracias por su apoyo.

Jhon Ríñger MELENDEZ MELENDEZ

Correo: jhon.melendez@unmsm.edu.pe, jhonmelendezm@gmail.com

Celular: 989108809

2) Dr. Frank Edmundo Escobedo Bailon



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

DOCTORADO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TÍTULO DE TESIS: "Modelo Sectrabank para Mitigar el Fraude Informático en Operaciones Electrónicas a través de Aplicaciones Bancarias en Dispositivos Android"

AUTOR: Jhon Rigner MELENDEZ MELENDEZ

ASESOR: Dr. Jorge Víctor MAYHUASCA GUERRA

APELLIDOS Y NOMBRES DEL JUEZ:	ESCOBEDO BAILON FRANK EDMUNDO
DNI:	41671087
FORMACIÓN ACADÉMICA:	DOCTOR EN INGENIERÍA DE SISTEMAS DOCTOR EN EDUCACIÓN DOCTOR EN PSICOLOGÍA
ÁREA DE EXPERIENCIA PROFESIONAL:	DOCENTE
INSTITUCIÓN:	UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Firma del experto informante



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: V1 MARCO DE TRABAJO

N°	DIMENSIONES / INDICADORES	ÍTEMS/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
	DIMENSIÓN 1: Conocimiento y experiencia sobre fraude informático y su entorno		SI	NO	SI	NO	SI	NO	
1	Conocimiento de las operaciones bancarias	¿Usted realiza operaciones bancarias?	X		X		X		
2	Conocimiento de ataques específicos de fraude informático	¿Tienes conocimiento de los ataques de fraude informático en la modalidad de Fake App y SIM Swapping?	X		X		X		
3	Experiencia personal con el fraude informático	¿Usted, su entorno amical o familiar, ¿En alguna oportunidad ha sido víctima de fraude informático?	X		X		X		
4	Conciencia y experiencia previa en el reconocimiento de intentos de fraude informático mediante técnicas de ingeniería social.	¿Ha recibido mensajes sospechosos relacionados con operaciones bancarias (phishing, smishing)?	X		X		X		
5	Nivel de conocimiento sobre herramientas tecnológicas avanzadas aplicadas a la seguridad bancaria.	¿Está familiarizado con el término "geolocalización" para la seguridad bancaria?	X		X		X		
6	Interés en fortalecer sus habilidades y conocimientos sobre prevención de fraudes.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
7	Intención de adopción de tecnologías específicas para la protección contra fraudes informáticos.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
	DIMENSIÓN 2: Usabilidad y percepción de aplicaciones bancarias con el modelo propuesto		SI	NO	SI	NO	SI	NO	
8	Percepción del usuario respecto al UX del modelo sectrabank	¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular?	X		X		X		
9	Percepción de confianza en la seguridad de las transacciones	¿Qué tan seguro se siente al realizar transferencias de gran monto por aplicaciones móviles?	X		X		X		



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

N.º	DIMENSIONES / INDICADORES	ÍTEM/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
			SI	NO	SI	NO	SI	NO	
	electrónicas realizadas mediante aplicaciones móviles.								
10	Conocimiento de buenas prácticas en la instalación y uso seguro de aplicaciones móviles.	¿Piensa que la instalación de aplicaciones desde fuentes oficiales reduce el riesgo de fraude?	X		X		X		
	DIMENSIÓN 3: Evaluación del modelo propuesto		SI	NO	SI	NO	SI	NO	
11	Evaluación sobre la eficacia del modelo en casos de Fake App	¿Considera que el modelo propuesto ha mitigado el ataque simulado de Fake App ejecutado en su dispositivo móvil?	X		X		X		
12	Evaluación sobre la eficacia del modelo en casos de SIM Swapping	¿Considera que el modelo propuesto ha mitigado el ataque simulado de SIM Swapping ejecutado en su dispositivo móvil?	X		X		X		
13	Disposición para usar la aplicación	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?	X		X		X		
14	Percepción de impacto del modelo en la eficiencia operativa de las transacciones bancarias.	¿Considera que el modelo propuesto afecta la velocidad de las transacciones?	X		X		X		
15	Opinión del usuario sobre la eficacia de las medidas de seguridad basadas en autenticación biométrica y características del dispositivo.	¿Es suficiente el uso del DMEI y huella dactilar para proteger las operaciones bancarias?	X		X		X		
16	Disposición de los usuarios para adoptar soluciones tecnológicas que incorporen el modelo de mitigación de fraudes.	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?	X		X		X		

Muchas gracias por su apoyo.

Jhon Rigner MELENDEZ MELENDEZ

Correo: jhon_melendez@unmsm.edu.pe, ihonmelendezm@gmail.com

Celular: 989108809

3) Dr. Luis Antonio Rivera Escriba



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

DOCTORADO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TÍTULO DE TESIS: "Modelo Sectrabank para Mitigar el Fraude Informático en Operaciones Electrónicas a través de Aplicaciones Bancarias en Dispositivos Android"

AUTOR: Jhon Rigner MELENDEZ MELENDEZ

ASESOR: Dr. Jorge Victor MAYHUASCA GUERRA

APELLIDOS Y NOMBRES DEL JUEZ:	RIVERA ESCRIBA LUIS ANTONIO
DNI:	06445707
FORMACIÓN ACADÉMICA:	DOCTOR EN CIENCIA DE LA COMPUTACIÓN
ÁREA DE EXPERIENCIA PROFESIONAL:	DOCENTE
INSTITUCIÓN:	UNIVERSIDAD ESTADUAL DO NORTE FLUMINENSE (UENF), BRASIL

Firma del experto informante



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: V1 MARCO DE TRABAJO

N.º	DIMENSIONES / INDICADORES	ÍTEMS/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
			SI	NO	SI	NO	SI	NO	
	DIMENSIÓN 1: Conocimiento y experiencia sobre fraude informático y su entorno		X						
1	Conocimiento de las operaciones bancarias	¿Usted realiza operaciones bancarias?	X		X		X		
2	Conocimiento de ataques específicos de fraude informático	¿Tienes conocimiento de los ataques de fraude informático en la modalidad de Fake App y SIM Swapping?	X		X		X		
3	Experiencia personal con el fraude informático	¿Usted, su entorno amical o familiar, ¿En alguna oportunidad ha sido víctima de fraude informático?	X		X		X		Usted o su entorno familiar o amical,
4	Conciencia y experiencia previa en el reconocimiento de intentos de fraude informático mediante técnicas de ingeniería social.	¿Ha recibido mensajes sospechosos relacionados con operaciones bancarias (phishing, smishing)?	X		X		X		
5	Nivel de conocimiento sobre herramientas tecnológicas avanzadas aplicadas a la seguridad bancaria.	¿Está familiarizado con el término "geolocalización" para la seguridad bancaria?	X		X		X		
6	Interés en fortalecer sus habilidades y conocimientos sobre prevención de fraudes.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
7	Intención de adopción de tecnologías específicas para la protección contra fraudes informáticos.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		¿Desearía adoptar un herramienta tecnológica para prevención defraudes informáticos?
	DIMENSIÓN 2: Usabilidad y percepción de aplicaciones bancarias con el modelo propuesto		SI	NO	SI	NO	SI	NO	
8	Percepción del usuario respecto al UX del modelo sectrabank	¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular?	X		X		X		¿Usted considera el aplicativo bancario instalado en su celular fácil de usar?
9	Percepción de confianza en la seguridad de las transacciones	¿Qué tan seguro se siente al realizar transferencias de gran monto por aplicaciones móviles?	X		X		X		¿Usted confía en realizar transferencias de valores por aplicaciones de celular?



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

N.º	DIMENSIONES / INDICADORES	ÍTEMS/PREGUNTAS	Claridad y lenguaje adecuado en la redacción	Mide lo que pretende	Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
	electrónicas realizadas mediante aplicaciones móviles.						
10	Conocimiento de buenas prácticas en la instalación y uso seguro de aplicaciones móviles. DIMENSIÓN 3: Evaluación del	¿Piensa que la instalación de aplicaciones desde fuentes oficiales reduce el riesgo de fraude?	X	X	X		
11	Evaluación sobre la eficacia del modelo en casos de Fake App	¿Considera que el modelo propuesto ha mitigado el ataque simulado de Fake App ejecutado en su dispositivo móvil?	SI	NO	SI	NO	¿Considera que el aplicativo SectraBank instalado en celular ha mitigado el ataque simulado de Fake App?
12	Evaluación sobre la eficacia del modelo en casos de SIM Swapping	¿Considera que el modelo propuesto ha mitigado el ataque simulado de SIM Swapping ejecutado en su dispositivo móvil?	X	X	X		¿Considera que el aplicativo SectraBank instalado en celular ha mitigado el ataque simulado de SIM Swapping?
13	Disposición para usar la aplicación	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?	X	X	X		
14	Percepción de impacto del modelo en la eficiencia operativa de las transacciones bancarias.	¿Considera que el modelo propuesto afecta la velocidad de las transacciones?	X	X	X		
15	Opinión del usuario sobre la eficacia de las medidas de seguridad basadas en autenticación biométrica y características del dispositivo.	¿Es suficiente el uso del IMEI y huella dactilar para proteger las operaciones bancarias?	X	X	X		
16	Disposición de los usuarios para adoptar soluciones tecnológicas que incorporen el modelo de mitigación de fraudes.	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?	X	X	X		

Muchas gracias por su apoyo.

Jhon Rigner MELENDEZ MELENDEZ

Correo: jhon.melendez@unmsm.edu.pe, jhonmelendezm@gmail.com

Celular: 989108809

4) Dr. Luis Alberto Vives Garnique



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

DOCTORADO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TÍTULO DE TESIS: "Modelo Sectrabank para Mitigar el Fraude Informático en Operaciones Electrónicas a través de Aplicaciones Bancarias en Dispositivos Android"

AUTOR: Jhon Rigner MELENDEZ MELENDEZ

ASESOR: Dr. Jorge Victor MAYHUASCA GUERRA

APELLIDOS Y NOMBRES DEL JUEZ:	VIVES GARNIQUE LUIS ALBERTO
DNI:	42462867
FORMACIÓN ACADÉMICA:	DOCTOR EN EDUCACIÓN
ÁREA DE EXPERIENCIA PROFESIONAL:	DOCENTE
INSTITUCIÓN:	UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS


Firma del experto informante



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: V1 MARCO DE TRABAJO

N°	DIMENSIONES / INDICADORES	ÍTEMS/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
			SI	NO	SI	NO	SI	NO	
	DIMENSIÓN 1: Conocimiento y experiencia sobre fraude informático y su entorno		SI	NO	SI	NO	SI	NO	
1	Conocimiento de las operaciones bancarias	¿Usted realiza operaciones bancarias?	X		X		X		
2	Conocimiento de ataques específicos de fraude informático	¿Tienes conocimiento de los ataques de fraude informático en la modalidad de Fake App y SIM Swapping?	X		X		X		
3	Experiencia personal con el fraude informático	¿Usted, su entorno amical o familiar, ¿En alguna oportunidad ha sido víctima de fraude informático?	X		X		X		
4	Conciencia y experiencia previa en el reconocimiento de intentos de fraude informático mediante técnicas de ingeniería social.	¿Ha recibido mensajes sospechosos relacionados con operaciones bancarias (phishing, smishing)?	X		X		X		
5	Nivel de conocimiento sobre herramientas tecnológicas avanzadas aplicadas a la seguridad bancaria.	¿Está familiarizado con el término "geolocalización" para la seguridad bancaria?	X		X		X		
6	Interés en fortalecer sus habilidades y conocimientos sobre prevención de fraudes.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
7	Intención de adopción de tecnologías específicas para la protección contra fraudes informáticos.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
	DIMENSIÓN 2: Usabilidad y percepción de aplicaciones bancarias con el modelo propuesto		SI	NO	SI	NO	SI	NO	
8	Percepción del usuario respecto al UX del modelo sectrabank	¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular?	X		X		X		
9	Percepción de confianza en la seguridad de las transacciones	¿Qué tan seguro se siente al realizar transferencias de gran monto por aplicaciones móviles?	X		X		X		

5) Dr. Marco Remigio Pusdá Chulde



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

DOCTORADO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TÍTULO DE TESIS: "Modelo Sectrabank para Mitigar el Fraude Informático en Operaciones Electrónicas a través de Aplicaciones Bancarias en Dispositivos Android"

AUTOR: Jhon Rigner MELENDEZ MELENDEZ

ASESOR: Dr. Jorge Victor MAYHUASCA GUERRA

APELLIDOS Y NOMBRES DEL JUEZ:	PhD. PUSDÁ CHULDE MARCO REMIGIO
DNI:	0401200951
FORMACIÓN ACADÉMICA:	DOCTORA EN CIENCIAS INFORMÁTICAS
ÁREA DE EXPERIENCIA PROFESIONAL:	DOCENTE
INSTITUCIÓN:	UNIVERSIDAD TÉCNICA DEL NORTE

MARCO
REMIGIO
PUSDA CHULDE

Firmado digitalmente
por MARCO REMIGIO
PUSDA CHULDE
Fecha: 2025.01.22
20:12:06 -05'00'

Firma del experto informante



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: V1 MARCO DE TRABAJO

N.º	DIMENSIONES / INDICADORES	ÍTEMES/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
	DIMENSIÓN 1: Conocimiento y experiencia sobre fraude informático y su entorno		SI	NO	SI	NO	SI	NO	
1	Conocimiento de las operaciones bancarias	¿Usted realiza operaciones bancarias utilizando dispositivos móviles?	X		X		X		
2	Conocimiento de ataques específicos de fraude informático	¿Tiene conocimiento de los ataques de fraude informático en la modalidad de Fake App y SIM Swapping?	X		X		X		
3	Experiencia personal con el fraude informático	¿Usted, su entorno amical o familiar, ¿En alguna oportunidad ha sido víctima de fraude informático?	X		X		X		
4	Conciencia y experiencia previa en el reconocimiento de intentos de fraude informático mediante técnicas de ingeniería social.	¿Ha recibido mensajes sospechosos relacionados con operaciones bancarias (phishing, smishing)?	X		X		X		
5	Nivel de conocimiento sobre herramientas tecnológicas avanzadas aplicadas a la seguridad bancaria.	¿Está familiarizado con el término "geolocalización" para la seguridad bancaria?	X		X		X		
6	Interés en fortalecer sus habilidades y conocimientos sobre prevención de fraudes.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
7	Intención de adopción de tecnologías específicas para la protección contra fraudes informáticos.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
	DIMENSIÓN 2: Usabilidad y percepción de aplicaciones bancarias con el modelo propuesto		SI	NO	SI	NO	SI	NO	
8	Percepción del usuario respecto al UX del modelo vnetbank	¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular?	X		X		X		
9	Percepción de confianza en la seguridad de las transacciones	¿Qué tan seguro se siente al realizar transferencias de gran monto por aplicaciones móviles?	X		X		X		



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

N.º	DIMENSIONES / INDICADORES	ÍTEMES/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
	electrónicas realizadas mediante aplicaciones móviles.								
10	Conocimiento de buenas prácticas en la instalación y uso seguro de aplicaciones móviles.	¿Piensa que la instalación de aplicaciones desde fuentes oficiales reduce el riesgo de fraude?	X	X	X	X	X	X	
DIMENSION 3: Evaluación del modelo propuesto									
11	Evaluación sobre la eficacia del modelo en casos de Fake App	¿Considera que el modelo propuesto ha mitigado el ataque simulado de Fake App ejecutado en su dispositivo móvil?	X	X	X	X	X	X	
12	Evaluación sobre la eficacia del modelo en casos de SIM Swapping	¿Considera que el modelo propuesto ha mitigado el ataque simulado de SIM Swapping ejecutado en su dispositivo móvil?	X	X	X	X	X	X	
13	Disposición para usar la aplicación	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?	X	X	X	X	X	X	
14	Percepción de impacto del modelo en la eficiencia operativa de las transacciones bancarias.	¿Considera que el modelo propuesto afecta la velocidad de las transacciones?	X	X	X	X	X	X	La velocidad no debería verse afectada al realizar transacciones mediante dispositivos móviles
15	Opinión del usuario sobre la eficacia de las medidas de seguridad basadas en autenticación biométrica y características del dispositivo.	¿Es suficiente el uso del DMEI y huella dactilar para proteger las operaciones bancarias?	X	X	X	X	X	X	
16	Disposición de los usuarios para adoptar soluciones tecnológicas que incorporen el modelo de mitigación de fraudes.	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?	X	X	X	X	X	X	

Muchas gracias por su apoyo.

Jhon Ríger MELENDEZ MELENDEZ

Correo: jhonmelendez@unmsm.edu.pe, jhonmelendezm@gmail.com

Celular: 989108809

6) Dr. Diego Miguel Marcillo Parra



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

DOCTORADO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TÍTULO DE TESIS: "Modelo Sectrabank para Mitigar el Fraude Informático en Operaciones Electrónicas a través de Aplicaciones Bancarias en Dispositivos Android"

AUTOR: Jhon Rigner MELENDEZ MELENDEZ

ASESOR: Dr. Jorge Victor MAYHUASCA GUERRA

APELLIDOS Y NOMBRES DEL JUEZ:	PHD DIEGO MIGUEL MARCILLO PARRA
DNI:	1710802925
FORMACIÓN ACADÉMICA:	DOCTOR EN TECNOLOGÍAS DE LA INFORMACIÓN Y SUS APLICACIONES
ÁREA DE EXPERIENCIA PROFESIONAL:	DOCENTE
INSTITUCIÓN:	UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE

DIEGO
MIGUEL
MARCILLO
PARRA

Firmado
digitalmente
por DIEGO
MIGUEL
MARCILLO
PARRA

Firma del experto informante



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: VI MARCO DE TRABAJO

N°	DIMENSIONES / INDICADORES	ÍTEMS/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
	DIMENSIÓN 1: Conocimiento y experiencia sobre fraude informático y su entorno		SI	NO	SI	NO	SI	NO	
1	Conocimiento de las operaciones bancarias	¿Usted realiza operaciones bancarias?	X		X		X		
2	Conocimiento de ataques específicos de fraude informático	¿Tiene conocimiento de los ataques de fraude informático en la modalidad de Fake App y SIM Swapping?	X		X		X		
3	Experiencia personal con el fraude informático	¿Usted, su entorno amical o familiar, ¿En alguna oportunidad ha sido víctima de fraude informático?		X	X		X		
4	Conciencia y experiencia previa en el reconocimiento de intentos de fraude informático mediante técnicas de ingeniería social.	¿Ha recibido mensajes sospechosos relacionados con operaciones bancarias (phishing, smishing)?	X		X		X		
5	Nivel de conocimiento sobre herramientas tecnológicas avanzadas aplicadas a la seguridad bancaria.	¿Está familiarizado con el término "geolocalización" para la seguridad bancaria?	X		X		X		
6	Interés en fortalecer sus habilidades y conocimientos sobre prevención de fraudes.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
7	Intención de adopción de tecnologías específicas para la protección contra fraudes informáticos.	¿Estaría dispuesto a asistir a capacitaciones sobre prevención de fraudes informáticos?	X		X		X		
	DIMENSIÓN 2: Usabilidad y percepción de aplicaciones bancarias con el modelo propuesto		SI	NO	SI	NO	SI	NO	
8	Percepción del usuario respecto al UX del modelo sectrabank	¿Considera usted que es amigable la aplicación bancaria mostrada e instalada en su teléfono celular?	X		X		X		
9	Percepción de confianza en la seguridad de las transacciones	¿Qué tan seguro se siente al realizar transferencias de gran monto por aplicaciones móviles?	X		X		X		



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA

N.º	DIMENSIONES / INDICADORES	ÍTEMS/PREGUNTAS	Claridad y lenguaje adecuado en la redacción		Mide lo que pretende		Esencial		OBSERVACIONES (Por favor, indique si debe eliminarse o modificarse algún ítem)
	electrónicas realizadas mediante aplicaciones móviles.								
10	Conocimiento de buenas prácticas en la instalación y uso seguro de aplicaciones móviles.	¿Piensa que la instalación de aplicaciones desde fuentes oficiales reduce el riesgo de fraude?	X		X		X		
	DIMENSIÓN 3: Evaluación del modelo propuesto		SI	NO	SI	NO	SI	NO	
11	Evaluación sobre la eficacia del modelo en casos de Fake App	¿Considera que el modelo propuesto ha mitigado el ataque simulado de Fake App ejecutado en su dispositivo móvil?	X		X		X		
12	Evaluación sobre la eficacia del modelo en casos de SIM Swapping	¿Considera que el modelo propuesto ha mitigado el ataque simulado de SIM Swapping ejecutado en su dispositivo móvil?	X		X		X		
13	Disposición para usar la aplicación	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?	X		X		X		
14	Percepción de impacto del modelo en la eficiencia operativa de las transacciones bancarias.	¿Considera que el modelo propuesto afecta la velocidad de las transacciones?	X		X		X		
15	Opinión del usuario sobre la eficacia de las medidas de seguridad basadas en autenticación biométrica y características del dispositivo.	¿Es suficiente el uso del IMEI y huella dactilar para proteger las operaciones bancarias?	X		X		X		
16	Disposición de los usuarios para adoptar soluciones tecnológicas que incorporen el modelo de mitigación de fraudes.	¿Estaría dispuesto(a) a utilizar la aplicación propuesta para mitigar los fraudes informáticos en las modalidades de SIM Swapping y Fake App?	X		X		X		

Muchas gracias por su apoyo.

Jhon Rigner MELENDEZ MELENDEZ

Correo: jhon.melendez@unmsm.edu.pe, jhonmelendezm@gmail.com

Celular: 989108809

Anexo 8 : Imágenes de encuestas a la DIVINDAT

En las tomas fotográficas 01 al 06), se observa a los efectivos policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT-DIRINCRI PNP), utilizando el modelo Sectrabank. En la fotografía No 01, se aprecia a un efectivo respondiendo la encuesta posterior a la prueba de uso. La evaluación fue realizada en las instalaciones de la DIVINDAT - DIRINCRI PNP, ubicadas en la Av. España N.º 323, Cercado de Lima. Por motivos de seguridad institucional, solo se han incluido algunas fotografías representativas del procedimiento.

Fotografía Nro. 01



Fotografía Nro. 02



Fotografía Nro. 03



Fotografía Nro. 04**Fotografía Nro. 05****Fotografía Nro. 06**

Anexo 9: Constancia de cantidad de efectivos policiales encargados de investigar delitos informáticos



POLICIA NACIONAL DEL PERÚ
DIRECCION DE INVESTIGACION CRIMINAL
División de Investigación de Delitos
de Alta Tecnología

CONSTANCIA

En atención a lo solicitado, por el señor JHON RIGNER MELENDEZ MELENDEZ, identificado con DNI N° 42151848 y con Código de Matrícula N° 21207122, alumno(a) del Programa de DOCTORADO EN INGENIERIA DE SISTEMAS E INFORMATICA, se informa que la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI PNP, es una unidad orgánica dependiente de la Dirección de Investigación Criminal y cuenta con **OCHENTA (80)**, efectivos policiales, entre varones y mujeres, con rango de edad entre los 24 a 50 años, que se encargan de Investigar Delitos Informáticos contemplados en la Ley 30096 y su Modificatoria Ley 30171 LEY DE DELITOS INFORMATIVOS, información que se remite al suscrito con fines académicos.

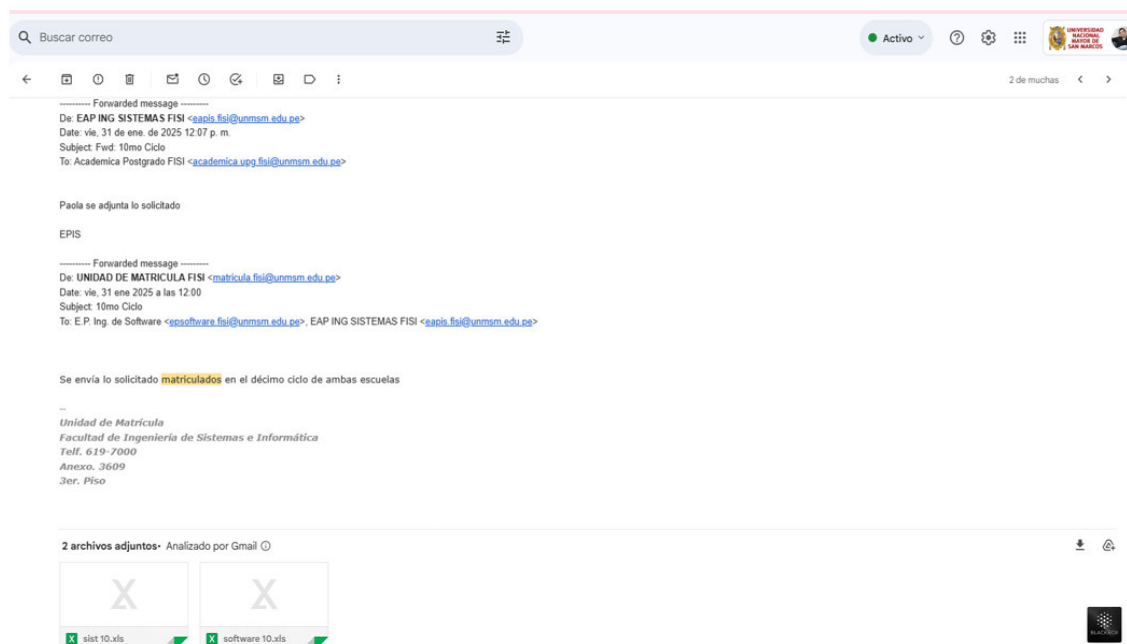
Lima, 06 de noviembre del 2024




OA-226633
Luis Edgardo HUAMAN SANTAMARIA
CORONEL PNP
JEFE DE LA DIVISION DE INVESTIGACION DE DELITOS
DE ALTA TECNOLOGIA - DIRINCRI PNP

Anexo 10: Constancia de cantidad de alumnos matriculados en decimo ciclo de ingeniería de software de la UNMSM

CORREO DE CONSTANCIA DE CANTIDAD DE ALUMNOS MATRICULADOS EN EL DÉCIMO CICLO DE INGENIERÍA DE SOFTWARE DE LA UNMSM



ARCHIVO ADJUNTO

Nº	cod_alumno	ape_paterno	ape_materno	nom_alumno	año_estudio	cod_citu	cod_perm	sede_alumno	cod_tip_ingreso
1	0095	IAS		MOISES	10	R	AC	---	SEB
2	0076	IC	DAÑA	SUSO	10	R	AC	---	SEP
3	0065	MEZ	AS	AUGUSTO	10	O	AC	---	SEB
4	0088	G	MEZ	S AUGUSTO	10	R	AC	---	TI
5	0067	ITALVO	CIA	Y ABEL	10	O	AC	---	SEB
6	0034	ASTIANI	AS	PIPER PAOLO	10	O	AC	---	SEB
7	0027		ERPEZ	EDUARDO	10	R	AC	---	SEB
8	0061	DAVE	TO	ETH JACQUELINE	10	R	AC	---	CEP
9	0096		AVENTE	AUGUSTO	10	O	AC	---	SEB
10	0048	ETO	NEA	ANGEL	10	R	AC	---	EBRA
11	0054	EDES	TES	TIANI	10	R	AC	---	EBRA
12	0082	ANCUY	NANDEZ	IN RICHARD	10	R	AC	---	EBRA
13	0089	S	RIQUEZ	RINE LESLY	10	R	AC	---	EBRA
14	0037	OJO		RINCK	10	R	AC	---	EBRA
15	0066	ORTO	OS	D GUSSEPI	10	R	AC	---	CEP
16	0038	AS	AS	D ALEXANDER	10	R	AC	---	CEP
17	0031	ALLAME	DOZ	IA CAROLINA	10	R	AC	---	PIR
18	0065	PRO	NANDEZ	ARLOS MIGUEL	10	R	AC	---	EBRA
19	0070	PERA	AS	OMAR	10	R	AC	---	EBRA
20	0097	SAREJO	RAJO	MEPPER	10	R	AC	---	EBRA
21	0097	AS	DOYA	DO MANUEL	10	O	AC	---	EBRA
22	0055	NUUEVA	CE	HANUEL	10	R	AC	---	EBRA
23	0058	TEROLA	DRAYME	NTONY	10	R	AC	---	EBRA
24	0051	LE	ATNEZ	ANDREA	10	R	AC	---	EBRA
25	0083	II	DO	IKARLA	10	R	AC	---	EBRA
26	0071	HE	SENTACIÓ	LEVIS	10	R	AC	---	EBRA
27	0078	RA	JOY	PRAYAN	10	R	AC	---	EBRA
28	0083	IA	IA	DO JUAN	10	R	AC	---	CEP
29	0088	ERES	MA	LUFONSO	10	R	AC	---	EBRA
30	0096	AN	FEDES	EL AARON	10	R	AC	---	EBRA
31	0000	NGO	FE	ALDA	10	R	AC	---	PPS
32	0005	OR	ENJO	IRIKELME	10	R	AC	---	EBRA
33	0019	IE	JUEZ	S AGRIAN	10	R	AC	---	EBRA
34	0022	EA	UAS	ROO DARIO	10	R	AC	---	CEP
35	0023	IA		MARTIN	10	R	AC	---	EBRA
36	0026	PREZ	TERO	ANTHONY	10	R	AC	---	CEP
37	0002	EZ	TIAGO	T WILLIAMS	10	R	AC	---	EBRA
38	0004	S	S	S ALONSO	10	R	AC	---	EBRA
39	0020	Z	RONES	XIMENA	10	R	AC	---	EBRA
40	0023	ENAS	PREZ	APLO	10	R	AC	---	EBRA
41	0024	UETA	EZ	ANDRES	10	R	AC	---	EBRA
42	0026	Z	IAS	ROO RODOLFO	10	R	AC	---	CEP
43	0023	BILLO	IA	IO JOSUE	10	R	AC	---	EBRA
44	0047	PREZ	RSAYA	RO SAUL	10	R	AC	---	EBRA
45	0048	RICIO	ITES	LUIS	10	R	AC	---	CEP
46	0055	INO	INO	ALEXANDRA	10	R	AC	---	EBRA
47	0056		AL	TIAN	10	R	AC	---	EBRA
48	0057	AZAMAM	AS	EDUARDO	10	R	AC	---	CEP
49	0064	UEZ	OMINO	JOSEPH	10	R	AC	---	EBRA
50	0066	EA	DO	L STACY	10	R	AC	---	EBRA
51	0067	SA	AS	MIGUEL	10	R	AC	---	EBRA
52	0069	ENNA	MANITUMA	NTONIO	10	R	AC	---	CEP
53	0070	HEA	ACRUZ	NOE	10	R	AC	---	EBRA
54	0071	VEZ	IPOS	IER	10	R	AC	---	EBRA
55	0097	ALA	CHEZ	ALONSO	10	R	AC	---	EBRA

Nº	cod_alumno	ape_paterno	ape_materno	nom_alumno	año_estudio	cod_citu	cod_perm	sede_alumno	cod_tip_ingreso
56	0002	ES	NUANA	AXEL	10	R	AC	---	EBRA
57	0028	AL	NIERO	MARTIN	10	R	AC	---	CEP
58	0029	RADO	OYO	AKIRA	10	R	AC	---	EBRA
59	0041	D	SAJO	IN SAMIR	10	R	AC	---	EBRA
60	0043	I	PARCO	L ALONSO	10	R	AC	---	EBRA
61	0043	A	ERPEZ	RODOLFO	10	R	AC	---	EBRA
62	0044	NO	SINCHO	D JHONATAN	10	R	AC	---	EBRA
63	0046		ACHO		10	R	AC	---	EBRA
64	0050	MEIRA	CA	ESTHER	10	R	AC	---	EBRA
65	0054	UTO	RES	FRIGLORA	10	R	AC	---	EBRA
66	0056	TEDES	PIA	R SEBASTIAN	10	R	AC	---	EBRA
67	0070		ES	ANGUEL	10	R	AC	---	EBRA
68	0073	NA	ITOYA	MANBRAYAN	10	R	AC	---	EBRA
69	0074	AL	NON	D ALFREDO RUBE	10	R	AC	---	EBRA
70	0076	HE	CHAR	NATONY	10	R	AC	---	EBRA
71	0081	PE	VDOO	IN ISMAEL	10	R	AC	---	EBRA
72	0082	PREZ	CIA	ARMANDO	10	R	AC	---	EBRA
73	0083	S	RIQUEZ	JACOB	10	R	AC	---	EBRA
74	0084	RA	KE	OFIBO	10	R	AC	---	EBRA
75	0090	D	MA	GENARO	10	R	AC	---	EBRA
76	0094	A	MAEVA	ESTANIN	10	R	AC	---	EBRA
77	0095	BILLO	UA	D JUNIOR	10	O	AC	---	EBRA
78	0098	DIA	ESAPAY	IR ALDAR	10	R	AC	---	EBRA
79	0002	RO	YO ALONSO		10	R	AC	---	EBRA
80	0003	SQUEZ		D RODRIG	10	R	AC	---	EBRA
81	0007	ANA	PAYA	A MARIA	10	R	AC	---	PPS
82	0016	CELO	NAS	ENRIQUE	10	R	AC	---	PPS
83	0011	TES	CZ	JUSTI	10	R	AC	---	PPS