



**Universidad Abierta
Interamericana**

**Ciberataques tipo Malware a usuarios de plataformas bancarias en
Argentina.**

Tutoría:

Profesora de Trabajo Final: Dra. Marcela Samela

Alumno: Daniela Romina Flores

Trabajo Final de Carrera

Lic. en Gestión de Tecnología Informática

- Diciembre 2024 -

Resumen

El objetivo de este trabajo final de carrera fue analizar los ciberataques dirigidos a usuarios de plataformas bancarias, utilizando un malware como herramienta principal. Los constantes avances tecnológicos y la creciente adopción de servicios bancarios digitalizados han generado un aumento significativo en la sofisticación y frecuencia de los ataques cibernéticos dirigidos a usuarios de instituciones financieras. El objetivo de esta investigación fue comprender las características y los riesgos asociados con los ciberataques por malware en las plataformas bancarias, así como proponer contramedidas eficaces para la mitigación de estos riesgos, y así evitar el impacto en los beneficios y la inmediatas de operar en las plataformas digitales de los bancos. El estudio se basó en una revisión exhaustiva de lo ya conocido e investigado sobre los ataques cibernéticos de tipo malware, así como en el análisis de casos reales a plataformas bancarias. Además, se exploraron las medidas de seguridad y protección implementadas por las entidades financieras, con el fin de robustecer la operatoria de los clientes y su confianza en el uso de las plataformas digitales, en pos de continuar avanzado en la digitalización financiera. Con base en los hallazgos de la investigación, se propusieron contramedidas y mejores prácticas para fortalecer la seguridad de los usuarios y sus dispositivos. Esto incluyo la implementación de sistemas de detección, autenticación de dos factores, educación y concientización de los usuarios, así como la colaboración entre las instituciones financieras y los organismos de seguridad cibernética.

Palabras clave: ciberataque, plataforma bancaria, riesgos, vulnerabilidades.

Abstract

The objective of this final degree project was to analyze cyberattacks directed to banking platforms users, using malware virus as the main tool. The continue Technological advances and the growing adoption of digitized banking services have generated a significant increase in the sophistication and frequency of cyber-attacks directed to financial institutions users. The objective of this research was to understand the characteristics and risks associated with cyberattacks by malware on banking platforms, as well as to propose effective countermeasures to mitigate those risks, and thus avoid the impact on benefits and the immediacy of operating on the banks' digital platforms. The study was based on an exhaustive review of what is already known and investigated about malware-type of cyber-attacks, as well as on the analysis of real cases involving banking platforms. In addition, all security and protection measures implemented by financial institutions were explored, in order to strengthen customer operations and strengthen their confidence in the use of digital platforms, for the purpose of continue progressing in financial digitization. Based on the research findings, countermeasures and best practices were proposed to strengthen the security of users and their devices. This included the implementation of detection systems, two-factor authentication, user education and awareness, as well as collaboration between financial institutions and cyber security agencies.

Keywords: cyberattack, homebanking, risks, vulnerabilities.

Dedicatoria

Dedico este trabajo final de carrera principalmente a Federico, mi pareja y compañero de viaje en la vida.

A mi familia, padres y hermanos, y a mis amigos que me acompañar durante este proceso, siendo mis sostén en los momentos de dificultad.

A mi jefe y compañeros de trabajo de HSBC, que apoyaron y acompañaron mis proceso de escritura, con ideas, vasto conocimiento y apoyo en las horas de dedicación.

A todas las personas involucradas directa o indirectamente en este trabajo: encuestados, autores, investigadores.

Reconocimientos

Este trabajo final de carrera es el cierre de una etapa de aprendizaje constante que es la facultad, donde uno pasa y dedica muchas horas de su vida, generando su propia trayectoria académica. Para lograrlo uno sacrifica momentos en su vida, tiempo valioso tanto físico como mental con el fin de llegar al objetivo final que es el tan ansiado título universitario. Año a año, materia a materia, fui experimentando todo tipo de sensaciones nervios, alegrías, aciertos, victorias, derrotas, frustraciones y miles de sensación que muchas veces me hacían sentir que había llega a mi limite, y que era un obstáculo que no iba a poder superar pero por suerte para mí, no camine este camino sola; sino que lo hice junto a mi pareja, familia, amigos de toda mi vida y fundamentalmente mi amigos de la facultad, todos ellos me empujaron a seguir, me apoyaron y me hicieron creer y entender que SI SE PUEDE, que con esfuerzo, perseverancia y dedicación se puede todo. Quiero agradecerles a todos ellos, y principalmente a Federico, quien se aguantó todos mis estados de ánimo y me apoyo de manera incondicional.

No quiero dejar de hacer un reconocimiento especialmente a mis compañeros y amigos de la facultad ya que sin ellos no podría haberlo logrado, recorrimos juntos toda la carrera y nos apoyamos incondicionalmente buscando siempre el bien común.

No puedo dejar de agradecer y reconocer a la Universidad Abierta Interamericana y sus profesores por los conocimientos y experiencias compartidas durante las clases. En especial a Marcela, profesora de trabajo final, quien dedica su tiempo y experiencia para enseñarnos día a día. Así, como a mis compañeros de la Facultad, de quienes aprendo y aprendí clase a clase.

A todos mencionados, y a todos los que formaron parte de mi trayecto universitario, les digo GRACIAS, vamos por más.

Índice

Resumen.....	1
Abstract	2
Dedicatoria	3
Reconocimientos	4
Índice de Tablas.....	8
Índice de Figura	9
1. Introducción	10
1.1 Planteamiento del Problema.....	11
1.2 Preguntas de la Investigación.....	12
1.3 Hipótesis.....	13
1.4 Justificación de la Propuesta	13
1.5 Objetivos	14
1.5.1 Objetivo General.....	14
1.5.2 Objetivos Específicos.....	14
1.6 Contribuciones Principales.....	14
1.7 Estructura General del Trabajo de Investigación	15
2.Estado del arte.....	16
3. Marco Teórico	17
3.1 Definición de ciberataques y su clasificación.	17
3.1.1 Ataque tipo malware: Mekotio.....	18
3.2 Descripción de las plataformas bancarias y su importancia en el sistema financiero.....	21
3.3 Marco Legal del ciberataque	22
3.4 Marco Regulatorio del ciberataque	23

3.5 Objetivos finales de los ciberataques -Malware.....	25
3.6 Ciberataques - Malware más comunes dirigidos a plataformas bancarias.....	26
4 Seguridad en plataformas bancarias.....	28
4.1 Ciberseguridad.	29
4.2 Metodologías de seguridad y protocolos actuales de protección de usuarios.....	29
4.3 Medidas de seguridad implementadas por las entidades financieras.	30
4.4 Estrategias y protocolos de seguridad de usuarios utilizados en América.	31
4.4.1 Afectación de ciberataques en el mundo.....	33
4.5 Campañas de concientización al usuario.....	36
5. Desarrollo Técnico.....	38
5.1 Introducción.....	38
5.2 Metodología de Investigación.....	38
5.2.1 Recopilación y análisis de datos.	39
5.3 Identificación y selección de casos de ciberataques malware.....	40
5.3.1 Emotet.....	40
5.3.2 Mekotio.....	40
5.3.3 Qbot (Qakbot).....	41
5.3.4 Conti.....	41
5.3.5 Ataques de Ransomware a organizaciones.....	41
5.3.6. Ramnit.....	42
6. Resultados.....	43
6.1 Análisis de los resultados obtenidos.....	43
6.1.1 Resultados obtenidos.....	43
6.1.2 Datos reales del impacto de la digitalización.....	49
6.2 Medidas de seguridad.....	53

7. Conclusiones	55
8. Líneas Futuras De Investigación.....	57
9. Referencias.....	58

Índice de Tablas

Tabla 1 Perfil Mekotio	19
Tabla 2 Puntuación en ciberseguridad.....	35
Tabla 3 Escala de países de América Latina	36
Tabla 4 Encabezado de la encuesta	47
Tabla 5 Clasificación de casuísticas detectada.....	49
Tabla 6 Cantidad de fraudes detectado.....	51

Índice de Figura

Figura 1 Detecciones de Mekotio en Latinoamérica (2023).....	20
Figura 2 Flujo de infección	27
Figura 3 Componentes de la estrategia de seguridad.....	30
Figura 4 Los 10 países con mayor riesgo de ciberamenazas	33
Figura 5 Mapa global de riesgo de ataque cibernético.....	34
Figura 6 Sitio de empresas de HSBC.....	37
Figura 7 Familia de malware que más afectaron América.	42
Figura 8 Respuestas pregunta 3	44
Figura 9 Respuestas pregunta 4	45
Figura 10 Respuestas pregunta 5	45
Figura 11 Respuestas pregunta 6.....	46
Figura 12 Respuestas pregunta 8	47
Figura 13 Respuestas de la pregunta 9.....	48
Figura 14 Ataques reportados por día	50
Figura 15 Reportes recibidos	51
Figura 16 Incremento de ciberataque por segmento de ciberataques por segmentó.....	52

1. Introducción

En la era digital en la que vivimos, los avances tecnológicos han transformado radicalmente la forma en que realizamos transacciones financieras. Las plataformas digitales se convirtieron en herramientas fundamentales para millones de personas en todo el mundo, brindando rapidez, facilidad, comodidad, eficiencia y accesibilidad a los servicios financieros. Sin embargo, esta creciente dependencia de la tecnología también ha generado nuevos desafíos y riesgos, convirtiéndose uno de los blancos más importantes y expuestos a los ciberataques.

Según Mc Afee (2023), un ciberataque por malware que afecta a una plataforma bancaria es la acción de un fraudulento o grupo de individuos fraudulentos que aprovechan a insertar un malware en la PC de los usuarios a través de las vulnerabilidades de los usuarios y/o de los sistemas informáticos de las entidades, e intenta acceder ilegalmente a información confidencial o realizar transacciones fraudulentas con el fin de obtener ganancias financieras ilícitas comprometiendo la integridad y la confidencialidad de la información sensible de los usuarios. Estos ataques pueden tener consecuencias importantes y graves, tanto para los usuarios de los servicios bancarios como para las propias instituciones financieras.

En este trabajo final se examinaron los ciberataques a través de malware a los usuarios de las plataformas bancarias, analizando sus diferentes tipos, métodos y las posibles medidas de mitigación que deben implementarse para prevenir y contrarrestar estos ataques, evitando generar un retroceso en la digitalización de la operatoria financiera y un gran impacto económico, que pueda afectar la sustentabilidad de dichas plataformas. Además, se exploraron los factores que contribuyen a una posible vulneración a los usuarios de las plataformas bancarias, como la falta de conciencia de seguridad, la ingeniería social, y las debilidades en los sistemas de autenticación.

A lo largo de esta investigación, se estudiaron casos reales de ciberataques por malware a plataformas bancarias que han ocurrido, como así el análisis de las tendencias actuales en términos de técnicas y estrategias utilizadas por los ciberdelincuentes. Además, se examinaron las regulaciones y normativas vigentes en materia de seguridad cibernética para evaluar su eficacia.

En concordancia por lo aseverado por la consultora Cloud.gal (2023) es fundamental comprender la importancia de abordar y mitigar los ciberataques a los usuarios de las plataformas bancarias, no solo para proteger los intereses financieros de los usuarios y las instituciones

bancarias, sino también para preservar la confianza en los servicios digitales y mantener la estabilidad del sistema financiero.

En el año 2020, ya se comenzaron a detectar sitios falsos, la Cámara Argentina de Comercio (2020) asevera que “5000 sitios falsos fueron registrados el 20 de marzo de este año y desde allí, 2000 sitios falsos siguen detectándose cada día” (p.1). Y a medida que avanzamos hacia una sociedad cada vez más digitalizada, más imprescindible es que se realicen estudios en materia de seguridad digital y se adopten medidas efectivas para fortalecer la seguridad cibernética en el sector bancario. El propósito de este trabajo final es aportar a este objetivo mediante un análisis exhaustivo de los ciberataques de tipo malware dirigidos a usuarios de plataformas bancarias. Se busca promover la conciencia, contribuir con recomendaciones prácticas y generar una comprensión profunda que pueda fortalecer la protección financiera en el entorno digital.

Con este propósito, el trabajo de investigación aborda inicialmente un marco conceptual que describe los principales conocimientos de la problemática de malware y cuales otros métodos de ataque se combinan con este, lo que se sabe en la actualidad de cada uno de ellos y como influyen intentando generar una des digitalización bancaria. A partir de ese contexto, se expone el desarrollo técnico de la investigación, sus correspondientes resultados, conclusiones y sugerencias sobre posibles trabajos futuros.

1.1 Planteamiento del Problema

En la actualidad, el uso generalizado de plataformas bancarias digitales se ha instalado como un gran beneficio que los bancos le brindan a los usuarios, así como la comodidad de realizar transacciones financieras desde cualquier lugar y en cualquier momento. Sin embargo, como comenta Camila Acosta (2022) en su artículo sobre los principales riesgos de la digitalización bancaria, esta creciente migración de los procesos u operatoria presencial a digital también ha dado lugar a un aumento significativo en los ciberataques dirigidos a los usuarios de las plataformas bancarias, lo que plantea un serio problema de seguridad.

Estos ataques son llevados a cabo por ciberdelincuentes que buscan acceder de manera ilícita a información confidencial, como datos personales y bancarios (ej. Contraseñas, token, números de tarjeta, códigos de seguridad, etc.), con el fin de realizar transacciones fraudulentas, como por ejemplo robar el dinero o cometer fraudes financieros (ej.: toma de un préstamo, alta de tarjeta de crédito, etc.).

La gran problemática de los ciberataques a través de malware son las importantes pérdidas financieras que los usuarios que pueden sufrir debido a transacciones fraudulentas o extorsión por parte de los atacantes. Además, estos ataques pueden dar lugar al robo de identidad, comprometiendo la privacidad de los usuarios y exponiéndolos a riesgos financieros y legales.

Por otro lado, según Adolfo José Dzigciot (2022) las instituciones financieras también enfrentan importantes desafíos frente a esta problemática, ya que los ataques exitosos pueden resultar en el descontento y pérdida de los clientes afectados, quienes podrían optar por cambiar a otras instituciones más seguras, incluso cuando los sistemas del banco no fueron vulnerados, sino que lo que se vulneró fue la computadora del usuario, generando un impacto financiero significativo y dañando la reputación de la institución afectada.

La casuística de ataque por medio de malware, según la empresa Cyberzaintza (2023), radica en la capacidad de los ciberdelincuentes para explotar las vulnerabilidades de los usuarios y de los equipos por los que acceden a las plataformas bancarias, ya sea a través de técnicas sofisticadas de hacking, ingeniería social, malware o phishing, entre otros métodos combinados; generando graves consecuencia tanto para los usuarios individuales como para las instituciones financieras.

Además, la constante y rápida evolución de la tecnología y de las prácticas de los ciberdelincuentes dificulta mucho más detección temprana y prevención de estos ataques. Los fraudulentos emplean constantemente nuevas tácticas y técnicas de robo de información sensible, lo que pone a los usuarios y a las instituciones bancarias en una carrera constante para mantenerse al día con las últimas amenazas y la protección de sus datos y sistemas.

En línea con el contexto actual, es fundamental abordar el problema de los ciberataques de malware a plataformas bancarias de manera integral y efectiva. Se requiere una comprensión profunda sobre los malware bancarios y los diferentes tipos de ataques que se combinan, para lograr detectar y proponer medidas de seguridad preventivas que ayuden a mitigar sus efectos. Asimismo, es necesario promover la concientización en materia de seguridad de la información entre los usuarios y establecer procesos para intentar garantizar la protección de la información tanto personal como financiera y la estabilidad del sistema bancario.

1.2 Preguntas de la Investigación

¿Cuáles son los principales métodos de propagación de malware utilizados para perpetrar fraudes en entornos bancarios digitalizados?

¿Cuál es la manera más efectiva de detectar y prevenir eficazmente los ataques de malware en las plataformas bancarias, especialmente con el crecimiento exponencial de dichos ataques?

1.3 Hipótesis

A partir de lo hasta aquí expuesto, podemos plantear las siguientes hipótesis, que luego será validas o refutadas en consecuencia:

- El aumento de los fraudes por casuística de malware creció exponencialmente con la digitalización bancaria.

1.4 Justificación de la Propuesta

La elección de investigar sobre ciberataques de tipo malware a plataformas bancarias se basa en la importancia y relevancia que este tema tiene en el actualidad en el sector financiero y en el camino hacia la digitalización bancaria, ya que su crecimiento fue exponencial. A continuación, mencionare algunos de los impactos generados:

Según explica Veritas Technologies (2022) el impacto significativo, hace referencia a la constante amenaza y evolución de los ciberataques de malware a plataformas bancarias, los cuales pueden tener consecuencias financieras y de seguridad graves tanto para los usuarios individuales como para las instituciones financieras. Estos ataques pueden resultar en la pérdida de dinero, el robo de identidad, la interrupción de los servicios bancarios y el daño a la reputación de las entidades financieras.

También menciona, el efecto social , ya que las plataformas bancarias son utilizadas en todo el mundo y se han convertido en una parte fundamental en la cotidianidad de las personas. La confianza en la seguridad y la integridad de estas plataformas es fundamental para el correcto funcionamiento del sistema financiero y la estabilidad económica en general.

Por otro lado, tenemos la constante evolución de las amenazas. Los ciberdelincuentes están constantemente desarrollando nuevas técnicas y herramientas para llevar a cabo ciberataques más sofisticados y difíciles de detectar. Es necesario investigar y comprender estas tendencias emergentes para poder anticiparse a ellas y desarrollar medidas de seguridad efectivas.

1.5 Objetivos

1.5.1 Objetivo General

El presente trabajo posee como principal objetivo proponer medidas de seguridad que ayuden a mitigar los riesgos y afectaciones que generan los ataques de Malware en las plataformas bancarias.

1.5.2 Objetivos Específicos

En cuanto a los diferentes objetivos específicos que se perseguirá durante el trabajo de investigación podemos mencionar los siguientes:

Evaluar las casuísticas de ciberataques por medio de malware dirigidos a los usuarios de las plataformas bancarias

Analizar el ciberataque de tipo malware(Mekotio) que está afectando a los usuarios de las plataformas bancarias en la actualidad.

Exponer las diferentes técnicas de ciberataques que los delincuentes emplean para atacar las plataformas bancarias.

1.6 Contribuciones Principales

El trabajo final de carrera proporcionará una visión integral y profunda sobre los diferentes tipos de ciberataques malware dirigidos a los usuarios de las plataformas bancarias. Se analizará en detalle las características, métodos y herramientas empleadas por los ciberdelincuentes en estos ataques. Este enfoque permitirá una comprensión profunda de las amenazas que enfrentan tanto las instituciones financieras como los usuarios individuales.

Se abordarán diferentes modalidades de malware, desde el phishing y ransomware hasta los ataques de ingeniería social, destacando sus modus operandi y cómo impactan en la seguridad y la confianza en las transacciones bancarias digitales. Además, se explorará la evolución de estas amenazas, proporcionando un panorama actualizado de los desafíos que deben abordar las entidades financieras y los usuarios.

Al profundizar en estos aspectos, el trabajo no solo buscará informar sobre las tácticas utilizadas por los ciberatacantes, sino también ofrecerá recomendaciones prácticas y estratégicas para mejorar la protección cibernética tanto a nivel institucional como individual. Este conocimiento integral será fundamental para fortalecer las defensas contra los ataques cibernéticos

en el sector bancario y promover una mayor conciencia sobre la seguridad digital entre todos los actores involucrados.

1.7 Estructura General del Trabajo de Investigación

A continuación, se precisa un resumen del contenido del trabajo de investigación y una breve descripción de cada uno de los 6 capítulos que lo componen.

En el capítulo 1. Introducción: se genera una introducción al tema elegido para la investigación, exponiendo el problema detectado, las hipótesis planteadas y los objetivos de la investigación.

En el Caputo 2. Estado del arte: donde se describen los antecedentes de la temática hasta lo último que se conoce sobre la materia.

En el capítulo 3. Marco teórico: donde se expone todo lo que se conoce de los ataques por casuística de malware desde el inicio hasta hoy. Se expone el encuadre regulatorio y legal. Los objetivos de estos ataques.

En el capítulo 4.Seguridad en plataformas bancarias: Se detallas medidas tomadas por los usuarios y las especificadas por el banco central como requisito mínimo. También, se hace un análisis de cuan expuestos están los diferentes países a los ciberataques en comparación con Argentina.

En el capítulo 5.Desarrollo técnico: Se plantea la metodología de la investigación, y como se generó la recolección de datos que darán inicio al análisis planteado.

En el capítulo 6.Resultados: Dentro de este capítulo analizaremos los resultados obtenidos tanto de las encuestas, como así de la investigación propuesta para lograr una conclusión fehaciente.

En el capítulo 7.Conclusion: se expondrá la conclusión obtenida luego de la exhaustiva investigación realizada, en conjunto con diferentes recomendaciones y mejores a aplicar en el ámbito bancario digital.

En el capítulo 8. Líneas futuras de investigación: En este apartado expondremos algunos puntos de partida para futuras investigaciones, que nacen del análisis realizado.

En el capítulo 9. Referencias: se especifica con el correcto formato y orden toda la bibliografía utilizada para el trabajo de investigación.

2.Estado del arte

La historia de los ciberataques a plataformas bancarias está en una evolución constante que refleja la creciente digitalización y la sofisticación de las amenazas en línea. A continuación, se muestra un resumen de las etapas del desarrollo de estos ataques y su historia:

Década de 2000 - La dirección Nacional de Ciberseguridad (2021) detecta que se generó un gran aumento en la cantidad de ataques cibernéticos mucho más sofisticado utilizando las tipologías de Malware y Phishing. Surgieron botnets, redes de dispositivos comprometidos, que se utilizaban para enviar correos electrónicos de phishing masivos y lanzar ataques de denegación de servicio distribuido (DDoS) contra plataformas bancarias. El phishing se volvió una de las amenaza más importante, donde los atacantes engañaban a los usuarios de las plataformas bancarias para que les proporcionaran sus credenciales bancarias y datos personales.

Década de 2010 - Se detecto un gran aumento de la tipología: Troyanos Bancarios, según se explica en el artículo Faster Capital (2023), se volvieron una de las mayores amenazas para las instituciones financieras. Ej.: ZeuS, SpyEye, etc. Estos troyanos eran capaces de infectar sistemas, robar credenciales, interceptar comunicaciones y realizar transferencias fraudulentas.

Actualidad - Amenazas mucho más sofisticadas, combinando las diferentes tipologías como por ej.: phishing y malware. Mónica Avelino Olivera (2023) escritora de Silent4Business¹ explica que los ciberdelincuentes desarrollan y avanza en nuevas técnicas y herramientas para llevar a cabo ataques contra plataformas bancarias, tomando como principal objetivo de ataque a los usuarios y sus computadoras. La ingeniería social es una de las técnicas más utilizadas para el robo de información sensible. Por otro lado, la explotación de vulnerabilidades y la distribución de malware persisten como métodos comunes.

A lo largo de estas etapas, las instituciones financieras han tenido que fortalecer sus medidas de seguridad para proteger sus sistemas y datos, mientras que los atacantes han seguido evolucionando sus métodos y técnicas, apuntando lo ataques a un target diferente, los usuarios.

¹ *Silent4Business: servicios y consultoría de TI, Mexico.*

3. Marco Teórico

En este capítulo se desarrolla el concepto ciberataque, su historia y evolución. Luego, se realiza una revisión profunda de los ataques de tipo malware, en específico, Mekotio y las diferentes tácticas con las que se combinan para afectar a los usuarios y las entidades bancarias y como impactan en la digitalización. Finalmente, se estudian las herramientas y medios de prevención existentes según el análisis presentado en esta investigación, así como el marco regulatorio y legal de la temática.

3.1 Definición de ciberataques y su clasificación.

Los ciberataques se definen como: “Los ciberataques son intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas.” (IBM, 2023, p.1). Por ende, podemos entender, que son acciones llevadas a cabo por fraudulentos para acceder y dañar los sistemas informáticos, redes o dispositivos electrónicos para obtener información confidencial, causando daño tanto a los individuos afectados y/o a las organizaciones.

La clasificación de los ciberataques puede variar, pero a continuación se presentan algunas categorías comunes:

Belcic (2023) define el malware como un ataque que implica el uso de un software malicioso que se instala en un sistema sin el consentimiento del usuario. Esto puede incluir virus, gusanos, troyanos, ransomware y spyware. El malware se utiliza para robar información, controlar sistemas o cifrar datos con el objetivo de obtener un rescate.

Algunas de las cepas más dañinas de malware roban datos financieros y otra información confidencial, que se usa después para cometer fraudes, extorsiones y robo de identidad.

Según la afirmación de Belcic (2023), “El phishing es una de las estafas más antiguas y mejor conocidas de Internet. Podemos definirlo como un tipo de fraude en las telecomunicaciones que emplea trucos de ingeniería social para obtener datos privados de sus víctimas”(p.1). Debemos resaltar que los medios más utilizados para esta técnica son: los correos electrónicos falsos, los mensajes de texto y los sitios web fraudulentos.

Seguin & Latto(2023), definen al Ransomware como un tipo de malware que bloquea el acceso a archivos y sistemas informáticos para luego pedir el pago de un rescate a cambio de devolver el acceso. El ransomware recurre al cifrado para bloquear el acceso a los archivos

infectados, lo que hace que las víctimas no los puedan abrir ni usar. Los ataques que se hacen con este malware tienen como objetivo toda clase de archivos, desde documentos personales hasta aquellos que resultan esenciales para la marcha de una empresa.

También encontramos otros tipos de ataques cibernéticos como la inyección de código, que se caracterizan por insertar código malicioso en aplicaciones web o bases de datos para lograr obtener acceso no autorizado o realizar acciones no deseadas que generen perjuicio al dueño del sistema. Los comunes son SQL injection (inyección SQL) y XSS (cross-site scripting). Según informa la Cámara Valencia (2016): “El XSS, a diferencia del ataque a SQL, persigue al usuario y no al servidor. Implica la inyección de código malicioso en un sitio web, que se ejecuta en el navegador del usuario cuando este accede al mismo”(p.1).

A estos ataques, se le suman técnicas de captación de información como la ingeniería social, la cual tienen como objetivo principal manipular psicológicamente a las personas para obtener información o datos sensibles, personales o acceso no autorizado a sistemas confidenciales. Estos engaños se generan por diferentes medio como el teléfono, el engaño en persona o la explotación de la confianza del usuario, redes sociales o combinado con otras técnicas de hackeo.

Estas son solo algunas categorías comunes de ciberataques, pero las técnicas utilizadas están en constante evolución. Es importante tener en cuenta que los ciberataques pueden combinar varias técnicas y enfoques para lograr sus objetivos.

3.1.1 Ataque tipo malware: Mekotio.

Mekotio es un troyano bancario (tipo de malware) que se enfoca principalmente en atacar a los clientes de las instituciones financieras. Está diseñado para robar información sensible, como credenciales de inicio de sesión, detalles de tarjetas de crédito y/o cuentas, así como, toda información personal disponible. Este malware opera infectando las computadoras y/o dispositivos de los clientes a través de archivos adjuntos incluidos en correos electrónicos maliciosos, sitios web comprometidos u otros métodos de distribución comúnmente utilizados por ciberdelincuentes (ESET, 2023).

Según un estudio realizado en España “Mekotio fue detectado por primera vez en marzo de 2018 y, desde entonces, su código y funcionalidades han ido evolucionando, pero sin perder nunca el foco en su objetivo principal, la banca online” (Instituto Nacional de Ciberseguridad de España, 2021, P.7).

Tabla 1*Perfil Mekotio*

Información	Detalles
Tipo de malware	Troyano bancario
Nombre del malware	Mekotio
Primer hallazgo	Marzo de 2018
Método de infección	Phishing -> descarga de .zip -> instalación de .msi
Método de propagación	Phishing
Carga útil	Archivo en formato[.]msi
Países objetivo	Chile, Perú, Uruguay, Paraguay, Bolivia, Mexico, Argentina, Ecuador, Brasil, Colombia, España y Reino unido

Nota. Esta tabla muestra el detalle técnico del malware Mekotio.

Según explica Miguel Ángel Mendoza (2023) una vez que infecta el sistema, Mekotio en primer lugar, suele centrarse en detectar lo llamado *Keylogging* (registro de pulsaciones de teclas), es decir, detecta y registra las pulsaciones de teclas realizadas por el usuario, capturando información sensible como nombres de usuario, contraseñas y otras credenciales cuando el usuario inicia sesión en la plataforma bancaria. Luego, cuando el usuario ya está dentro de su sesión de home banking, Mekotio puede interceptar los datos introducidos, incluidos números de tarjetas de crédito, direcciones y otra información personal, así como también tomar capturas de la pantalla de la víctima, logrando obtener información valiosa que se muestra en la pantalla durante sesiones. Luego simula pantallas similares a la de las plataformas bancarias con información ficticia, de modo que el usuario cree estar sufriendo una actualización de seguridad de la institución financiera, cuando en realidad por detrás, Mekotio está generando operaciones fraudulentas dentro de la plataforma en nombre del usuario.

A su vez asegura que, el malware muestra ventanas emergentes falsas o mensajes en la pantalla de la víctima para engañarlos y hacer que proporcionen información adicional requerida

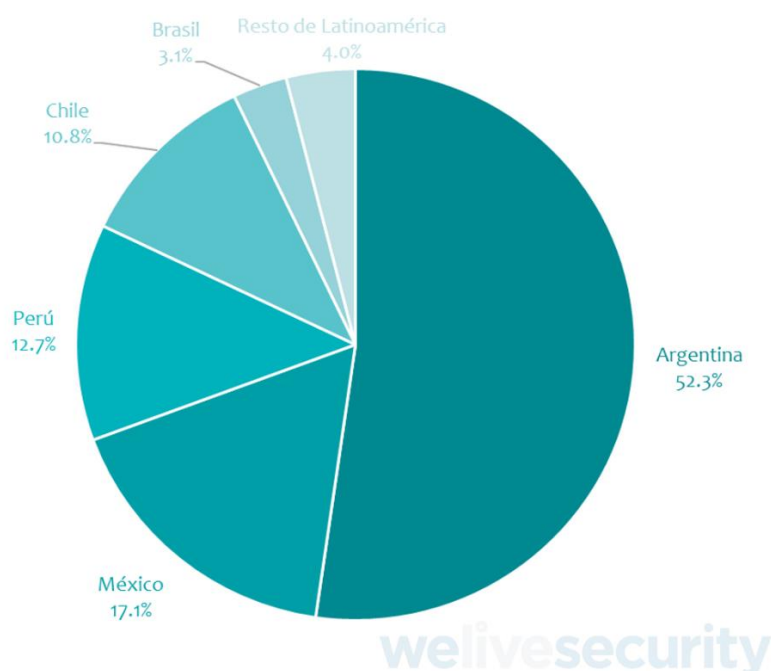
por el sistema como, códigos de autenticación del token, tarjeta de coordenadas y/o código de verificación enviados por el banco, etc.

De este modo, el malware logra su objetivo principal que es robar credenciales de inicio de sesión de cuentas de banca en línea, cuentas de correo electrónico y otros servicios para obtener acceso no autorizado a información sensible y realizar operaciones fraudulentas para robar el dinero de la víctima haciéndolo circular por cuentas mulas. En cuestión de minutos el dinero robado, circula por varias cuentas y desaparece del sistema financiero a través de la compra de criptomonedas o extracciones en sucursales bancarias.

A continuación, podemos ver el porcentaje de afectación del malware Mekotio en Latinoamérica por país impactado. También existen otros países fuera de Latinoamérica que se encuentran afectados por esta amenaza, como por ej.: España, Italia y Ucrania.

Figura 1

Detecciones de Mekotio en Latinoamérica (2023)



Nota. Tomado de las detecciones de Mekotio en Latinoamérica, de Miguel Ángel Mendoza, 2023, <https://www.welivesecurity.com/>, dominio público.

3.2 Descripción de las plataformas bancarias y su importancia en el sistema financiero.

Una plataforma bancaria digital, también conocida como “home banking” o banca electrónica, es una plataforma que permite a los clientes de instituciones financieras realizar diversas transacciones, gestionar sus productos y/o estar en contacto con su oficial o banco a través de Internet o aplicaciones móviles. Las plataformas digitales tienen como objetivo permitirles a los usuarios realizar todas sus gestiones bancarias sin tener que visitar una sucursal física (Banco Santander, 2023).

Dentro de sus funcionalidades más relevantes permite acceder a la visualización y administración de las cuentas/ tarjetas/ prestamos/ productos de inversión, etc., donde los clientes pueden ver información detallada sobre sus cuentas bancarias, incluyendo saldos, historiales de transacciones, resúmenes y detalle del producto. Así como también operar dichas cuentas realizando transferencias de fondos entre cuentas propias/ terceros mismo banco o interbancarias, pago de servicios o impuestos. También permite realizar inversiones, a través, de la compra/venta de acciones, moneda extranjera, invertir en fondos comunes de inversión o Plazo fijo, entre otros.

Según el centro de análisis Funcas (2020), con el correr de los años las plataformas bancarias se volvieron no solo transaccionales sino también relacionales y permitieron a los clientes utilizarlas como un medio de comunicación con el banco, dándole la posibilidad al cliente de contratar nuevo productos por los canales digitales, como también comunicarse a través de estas con su ejecutivo de cuenta o asesor financiero a través de un chat en línea o un inbox. Por otro lado, el cliente también puede configurar alertas, notificaciones y avisos, los cuales permiten mantenerse informados sobre transacciones y actividades en sus cuentas.

Todas las plataformas cuentan con diferentes medidas de seguridad implementadas por las entidades para asegurar la robustez y la confiabilidad de estas, como por ej.: doble factor de autenticación (token, tarjeta de coordenadas, etc.), cifrado de datos, enmascaramiento de datos sensibles, para proteger la información sensible de los clientes.

En coincidencia con lo mencionado por Accion.point (2023) el centro de todas las plataformas bancarias se encuentra cliente, especialmente cuando nos encontramos en un entorno competitivo y cambiante con la participación de competidores nuevos y tradicionales, pero ambos completamente digitales.

En los últimos años, según Forbes (2022), con la irrupción de las Fintech y la transformación digital de la banca tradicional, la innovación se ha convertido en una prioridad más

que nunca, ya que los bancos deben tener la capacidad de adaptar las plataformas a tecnologías flexibles y escalables de una manera ágil y automatizada sin dejar de lado la seguridad y la sustentabilidad. En esta búsqueda, la tecnología es un aliado esencial para lograrlo.

Por otro lado, y en concordancia con José Luis Portocarrero (2023) se comienza a darle mucha relevancia a los conceptos de Open Banking y Banking as a Service, no solo como una respuesta a las normativas regulatorias del ecosistema financiero, sino también como una oportunidad para aprovechar las capacidades de terceros y el ecosistema en general, con el objetivo de brindar los mejores y mayor cantidad de productos y servicios ya sea con capacidades internas o en colaboración con esos terceros para contribuir a la relación entre el cliente y cada entidad financiera.

3.3 Marco Legal del ciberataque

Los ciberataques a plataformas bancarias son ilegales en la mayoría de los países y están sujetos a diversas leyes y regulaciones relacionadas con la ciberseguridad, la privacidad de los datos y la protección de la infraestructura. Las leyes abarcan diferentes universos para proteger tanto a los usuarios como a las entidades afectadas, por un lado, encontramos leyes de fraudes y/o robos, protección de datos y regulaciones bancarias y, por otro lado, leyes antiterroristas o internacionales las cuales también aplican, ya que no necesariamente el ciberdelincuente o grupo atacante está en el mismo país donde se efectúa el ataque.

En Argentina contamos con leyes específicas de ciberseguridad que prohíben el acceso no autorizado a sistemas informáticos y redes, las cuales suelen establecer penas para quienes realicen ciberataques, incluyendo la prisión y multas. Algunas de las leyes y normativas relevantes dictadas por el Gobierno Argentino son las siguientes:

Ley de Entidades Financieras. Ley 21.526 (2021): Esta ley regula el funcionamiento de las entidades financieras en Argentina y establece ciertos requisitos y obligaciones relacionados con la seguridad de la información financiera y la confidencialidad de los datos de los clientes.

Ley de Delitos Informáticos. Ley 26.388 (2008): Esta ley aborda los delitos informáticos en Argentina y establece sanciones para actividades delictivas relacionadas con la informática, incluyendo el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones electrónicas y otros actos similares.

Regulación del Banco Central de Argentina: El Banco Central de Argentina emite regulaciones específicas relacionadas con la seguridad cibernética de las instituciones financieras bajo su jurisdicción. Estas regulaciones establecen estándares y requisitos de seguridad que los bancos deben cumplir para proteger sus sistemas y la información de los clientes.

Ley de Protección de Datos Personales. Ley 25.326 (2000): Esta ley establece los principios y requisitos para el tratamiento de datos personales en Argentina. Los bancos están sujetos a esta ley y deben tomar medidas para proteger la privacidad y seguridad de los datos personales de sus clientes.

Ley de Firma Digital. Ley 25.506 (2019): Esta ley regula la firma digital y la validez legal de los documentos electrónicos firmados digitalmente. Es relevante en el contexto de la seguridad de las transacciones bancarias en línea.

Es importante destacar que la aplicación de estas leyes y regulaciones puede variar dependiendo de la naturaleza y gravedad del ciberataque. Los bancos y las autoridades relevantes en Argentina colaboran estrechamente para investigar y perseguir a los responsables de ciberataques bancarios.

3.4 Marco Regulatorio del ciberataque

El Banco Central de la República Argentina (BCRA) ha emitido regulaciones y directrices relacionadas con la ciberseguridad para las entidades financiera, en estas regulaciones propone como objetivo principal proteger la integridad de los sistemas financieros y la información de los clientes. Las normas más importantes de cara a la entidades bancarias, usuarios y plataformas digitales son las siguientes:

Según BCRA (2023) se publicaron las Comunicación "A" 7783 y Comunicación "A" 7773, reemplazando a la normativa Com A 6017 y complementarias (2016):

La comunicación "A" 7783 establece los nuevos requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información asociados a los servicios financieros digitales para las Entidades Financieras y Proveedores de Servicios de Pago (PSP) de Argentina, alineándolos con los requisitos técnicos definidos en la Comunicación "A" 7777 de BCRA. En conjunto norman las pautas mínimas de ciberseguridad a cumplir por los canales digitales de las entidades financieras.

En esta comunicación el BCRA (2023) incentiva el uso adecuado y seguro de las operaciones financieras digitales y de sus datos, en el marco de tecnologías seguras, políticas de

privacidad claras y una gestión proactiva de la seguridad de la información. Además, establece una nueva base de Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con la tecnología informática y seguridad de la información, extendiendo su alcance a las infraestructuras del mercado financiero a fin de dar mayor cobertura en la gestión de riesgo de las operaciones realizadas por servicios financieros digitales, enfocados en aspectos de control y monitoreo de aquellas prestaciones de servicios a clientes por medios digitales que permitan efectuar al menos, transferencias, pagos, extracciones, consultas u otras operaciones en línea, permitidas por las regulaciones vigentes.

El BCRA (2023) hace hincapié en la evaluación de los riesgos referentes a la apertura de cuentas no presenciales de clientes, los factores de autenticación para el acceso y aprobación de instrucciones realizadas desde canales, debiéndose contar con los controles efectivos para la identificación y autenticación de los clientes al momento de transaccionar, limitando la exposición de los datos personales, validando la correspondencia de los dispositivos de uso con el cliente así como los puntos de contacto declarados.

Las entidades financieras deberán seguir elaborando planes de capacitación y concientización específicos para los servicios financieros digitales, proveyendo además, vías de comunicación 7x24 recepcionando consultas y denuncias, notificaciones de ciber incidentes y/o situaciones sospechosas que deben registrarse y analizarse en el marco de un proceso establecido para eventos de seguridad, incluyendo el monitoreo de técnicas de ingeniería social tanto para la empresa, como clientes y terceras partes (BCRA, 2023).

La Com A 7777 fue generada por BCRA con el texto ordenado sobre los Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información , donde se actualizan las prácticas y requisitos de seguridad dando forma al marco regulatorio completo con el objetivo de proteger al usuario de canales digitales en base a resiliencia operacional, preservando la estabilidad del sistema financiero. (BCRA 2023).

Según BCRA, la Comunicación "A" 6480 (2018) y “A” 6656 (2019) complementaria: Esta comunicación establece las pautas de ciberseguridad para las entidades financieras. Entre los aspectos que aborda se incluyen:

- La necesidad de contar con un responsable de seguridad de la información.
- La implementación de medidas de seguridad informática adecuadas para proteger la infraestructura tecnológica y los datos.

- La notificación obligatoria al BCRA de incidentes de seguridad cibernética significativos.
- La realización de auditorías internas y externas de seguridad cibernética.

El BCRA anualmente realiza las auditorías necesarias para asegurar el cumplimiento de los lineamientos establecidos por las normas publicadas, por ende, las entidades financieras están obligadas a cumplir con estas regulaciones y a tomar medidas para garantizar la seguridad de sus sistemas y la información confidencial de los usuarios.

3.5 Objetivos finales de los ciberataques -Malware.

El objetivo final de los ciberataques de malware a plataformas bancarias es obtener ganancias financieras ilícitas a través de una serie de técnicas de engaño y estrategias. La agencia de ciberseguridad Cyberzaintza (2023) asegura que los delincuentes que llevan a cabo estos ataques buscan aprovecharse de las vulnerabilidades en la seguridad de las instituciones financieras, así como, en las de los usuarios de las plataformas para obtener acceso no autorizado a cuentas bancarias, sistemas de pago, o información financiera confidencial a través de la instalación de un software malicioso en sus computadoras, con varios objetivos con un único fin.

La agencia de ciberseguridad Cyberzaintza (2023) también, asevera que el objetivo principal de los ciberataques a través de malware es el robo de fondos. Los atacantes buscan acceder a las cuentas bancarias de clientes o sistemas de transferencia de dinero para transferir fondos a cuentas mulas controladas por ellos. La cuenta mula se entiende como una cuenta que se abre para darle un uso fraudulento, utilizando datos verídicos robados para su apertura.

Para poder lograr su objetivo, los ciberdelincuentes buscan acceder a bases de datos que contengan información financiera y personal de los clientes, como números de tarjetas de crédito, números de seguridad social, contraseñas y otros datos sensibles. Al obtener esta información, la utilizan para cometer fraudes financieros adicionales.

A su vez, según informa la Secretaria de Innovación Tecnológica del sector público (2022), algunos ciberdelincuentes pueden intentar extorsionar a las instituciones financieras exigiendo un rescate a cambio de no divulgar información confidencial o de no lanzar ataques cibernéticos más destructivos que en algunos casos pueden generar interrupciones de los servicios, lo que puede causar pérdidas financieras a las instituciones y debilitar la confianza de los clientes en el sistema bancario.

Otro de los objetivos de los ataques es el mal uso de las cuentas bancarias robadas para realizar transacciones y transferencias de dinero con el fin de "lavar" dinero obtenido de actividades ilícitas.

Es importante destacar que los ciberataques a plataformas bancarias pueden variar en complejidad y alcance, y los motivos pueden ser financieros, políticos, ideológicos o una combinación de estos.

3.6 Ciberataques - Malware más comunes dirigidos a plataformas bancarias.

A lo largo de los años, ha habido varios casos de ataques de malware a entidades bancarias en todo el mundo. Estos casos han demostrado la sofisticación y la creciente amenaza que representan para el sector financiero. A continuación, menciono algunos casos testigos de ejemplos de malware a entidades bancarias:

Carbanak/Cobalt Group, año 2013-2018: Según Fernando Díaz periodista de Hispasec (2018), el grupo Carbanak, también conocido como Cobalt, llevó a cabo una serie de ataques cibernéticos a bancos en todo el mundo, robando más de mil millones de dólares durante varios años. Utilizaron malware personalizado para comprometer cajeros automáticos y sistemas bancarios internos.

Bangladesh Bank Heist, año 2016: En este caso digiALERT (2023) explica, los ciberdelincuentes utilizaron malware para comprometer el sistema de pagos del Banco Central de Bangladesh y robaron aproximadamente 81 millones de dólares. Aunque parte del dinero fue recuperado, el incidente resaltó la vulnerabilidad de las instituciones financieras a ataques cibernéticos.

Emotet, año 2020-2021: Según informa Mónica Tilves (2021) periodista del portal Silicon², Emotet es un troyano bancario que ha sido ampliamente utilizado en ataques cibernéticos dirigidos a bancos y entidades financieras en todo el mundo. Ha sido empleado para robar credenciales bancarias y propagar otros tipos de malware, incluyendo ransomware. (Pag.6)

Mekotio en Argentina, año 2018-2023: Según Basque cybersecurity centre (2021) Mekotio es una cepa de malware bancario, que surgió en marzo de 2018 y evoluciona continuamente tanto en sus objetivos como en sus capacidades. Inicialmente, Mekotio se centró en entidades bancarias

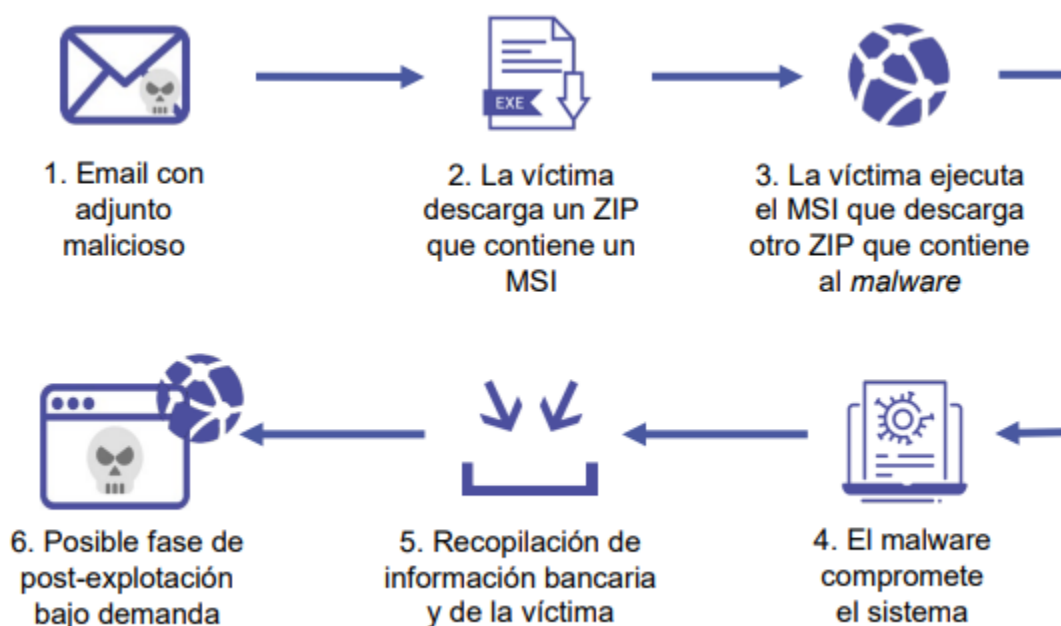
² Silicon: *fuentes de noticias en tecnología para empresas*

en Brasil, pero con el tiempo, expandió su alcance hacia otras regiones, incluyendo Chile, México, Colombia, España y Argentina, afectando a casi 50 instituciones financieras. (p.3)

En marzo de 2021, se detectó una campaña de correos fraudulentos particularmente intensa, diseñada con el propósito de persuadir a las víctimas para que descargaran este malware. Como explica el informe de Basque cybersecurity centre (2021), Mekotio demostró ser capaz de robar credenciales de banca en línea, comienza su operación recopilando información básica del equipo infectado y posteriormente la transmite al servidor de comando y control (C2C) utilizado por los atacantes. A partir de ahí, Mekotio se coloca en espera, activando una serie de temporizadores, esperando recibir instrucciones de los atacantes a través del servidor C2C. Estos temporizadores incluyen la detección de conexiones a través de navegadores web a sitios de entidades bancarias mediante la supervisión de las URL, la finalización de procesos del Administrador de Tareas en caso de que se detecten en funcionamiento, y la posibilidad de modificar el contenido. (p.3)

Figura 2

Flujo de infección



Nota. Tomado de MEKOTIO, Basque Cybersecurity centre, 2021, <file:///C:/Users/flore/Downloads/bcsc-malware-mekotio-tlpwhite816.pdf>

En abril del año 2023, Alejandro Musso, fiscal de la Unidad Fiscal Especializada en Investigaciones de Ciberdelito (UFEIC) de San Isidro afirmo que:

Hasta el momento, se sabían de casos de estafas virtuales por Mekotio en Brasil, Chile y México, pero no en nuestro país.

Las averiguaciones comenzaron luego que una concesionaria de venta de autos de alta gama denunciara el robo de un millón de pesos de sus cuentas bancarias.

De esta manera, se llegaron a rastrear a otras tres empresas a las cuales les sustrajeron 33, 12 y 15 millones de pesos, respectivamente; lo que hizo que los especialistas en ciberdelitos se dieran cuenta que los hackers se enfocaban en las cuentas bancarias de empresas donde saben qué hay depositada una mayor cantidad de dinero, que la que obtienen de un particular.(p.1)

Finalmente, los bancos y entidades financieras no responden a ningún reclamo, ya que ellos no tienen responsabilidad ni participación por quien dio acceso a un archivo nocivo en su propio dispositivo electrónico.

La recomendación para prevenir este tipo de estafas virtuales es nunca abrir ningún archivo adjunto de un mail que genera sospecha.

4 Seguridad en plataformas bancarias

En este apartado vamos a mencionar los protocolos y medidas de seguridad que actualmente tienen implementadas las entidades financieras para continuar analizando y detectando posibles mejoras o mitigantes.

4.1 Ciberseguridad.

La ciberseguridad se define como las buenas prácticas que se implementan o realizan para poder proteger todos los equipos o sistemas informáticos de cualquier ciberataque o amenaza para generar confianza entre los usuarios de las plataformas digitales.

De acuerdo a los expertos, la seguridad informática se define como, “ la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad de la tecnología de la información”(IBM,2023, p.1).

Según IBM (2023) esta función se encuentra en manos de expertos en seguridad informática, que trabajan con otro expertos para establecer múltiples capas de defensa contra las posibles amenazas, con el objetivo de diseñar un enfoque integral de seguridad e implementar medidas de protección en la organización.

4.2 Metodologías de seguridad y protocolos actuales de protección de usuarios.

Reconocer todos los riesgos que involucra la digitalización, no implica dejar de operar en línea, sino estar atentos a las diferentes medidas de seguridad para mantener seguras nuestras cuentas bancarias.

Según lo publicado por Lisa Institute (2019) hay 11 consejos los cuales pueden ser de ayuda para proteger tus operatoria digital. Entre ellos menciona el incluir nombre de usuarios y contraseñas los cuales sean fácil de recordar y difíciles de descifrar, con la inclusión de caracteres especiales y mayúsculas y generar cambio de manera asidua. Por otro lado, el uso de antivirus en todos los dispositivos mediante los cuales se operan las cuentas, así como doble factor (token, tarjeta de coordenada, validación biométrica) de autenticación para ingresar y realizar operaciones.

A su vez, Lisa Institute (2019) menciona la importancia de validar los links o direcciones a las que se ingresa, para asegurar que no son falsas, ya que suelen utilizar direcciones web muy similares a la real. Sumado al chequeo, menciona que es importante operar en redes seguras y no tener activado el bluetooth para evitar la filtración de datos o claves, así como, mantener siempre actualizadas las versiones de los dispositivos que generalmente traen mejoras en materia de seguridad.

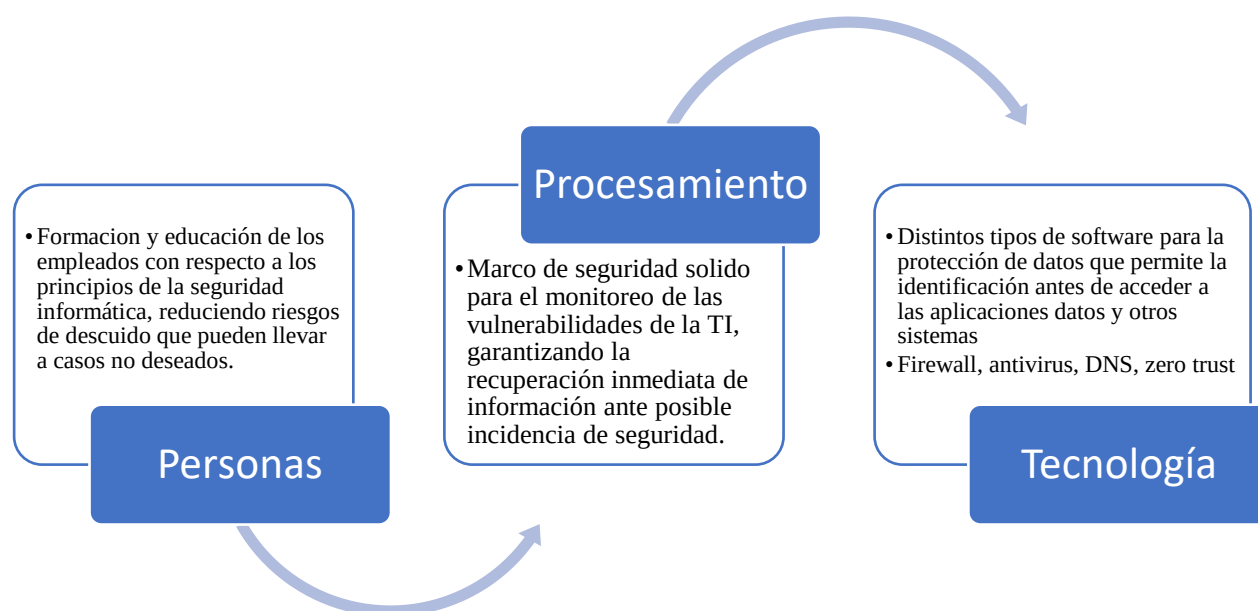
También menciona ciertas medidas de seguridad que los bancos están implementando y ofreciendo a los clientes en materia de seguridad como, por ejemplo, la opción de recibir alertas

por mail o SMS frente a cualquier movimiento o transacción realizada sobre las cuentas, así como la posibilidad de deshabilitar inicios de sesión automáticos. Sumado a estas alternativas, hay bancos que están implementado sistema de monitoreo de transacciones (Lisa Institute, 2019).

Por lo tanto, podemos definir 3 grandes componentes en la estrategia de seguridad:

Figura 3

Componentes de la estrategia de seguridad



Nota. Adaptado de la investigación de Amaquema Chuquiana Evelyn Maoli, 2023, análisis del ataque del modelo phishing en los sistemas informáticos bancarios.

4.3 Medidas de seguridad implementadas por las entidades financieras.

Para poder proponer mejoras, debemos tener en claro cuáles son las diferentes medidas o protocolos de seguridad que los bancos deben tener implementados en materia de seguridad de cara a sus usuarios. Según el Banco Central de la República Argentina y su Comunicación “A” 7783 hay requisitos mínimos de seguridad que todas las entidades bancarias deben cumplimentar.

El BCRA (2023) indica que para cumplir con los requisitos de seguridad y protección de datos, se establecen varias medidas y controles. Se requiere autenticación e identificación del cliente para realizar transacciones, utilizando métodos como usuario, clave, token (físico o digital), tarjeta de coordenadas e identificación biométrica. Además, se debe monitorear todas las transacciones críticas con un sistema de prevención de fraudes, estableciendo reglas para solicitar técnicas de autenticación multifactor en caso de coincidencia. Los datos sensibles deben permanecer cifrados durante toda la operación y no deben ser accesibles de manera simple en caso de ser interceptados. Se debe identificar cualquier cambio de dispositivo o chip del cliente y exigir autenticación positiva y multifactor para utilizar el dispositivo, evitando que un mismo usuario esté activo en más de una sesión. También se establecen controles específicos para los factores basados en secretos memorizados por los usuarios y los factores asociados a dispositivos únicos del cliente, como tokens OTP, tarjetas de coordenadas y tarjetas de crédito o débito (p. 6).

Además, las entidades deben proveer puntos de contacto, avisos, alertas y consejos de seguridad a los usuarios, ofreciendo la posibilidad de configurar alertas y/o avisos sobre sus cuentas y alertar sobre posibles comportamientos fraudulentos. Se deben actualizar los protocolos establecidos por la industria financiera y contar con un plan integral de datos que garantice el cumplimiento de protocolos y el manejo de brechas de seguridad. Se deben realizar auditorías anuales para asegurar el cumplimiento de todos los requisitos establecidos por el regulador, con evidencia que lo avale. Todos los sistemas y/o infraestructura de las entidades financieras deben estar actualizados, implementando los parches de seguridad y evitando vulnerabilidades. Todas las aplicaciones deben tener validaciones y permisos registrados y correctamente administrados, y todo ingreso a los sistemas debe hacerse al menos con usuario y clave, quedando registro de ingreso. (BCRA, 2023, p. 17)

4.4 Estrategias y protocolos de seguridad de usuarios utilizados en América.

América latina al igual que otros países del mundo, está viéndose afectada por los ciberataques, es uno de los continentes más afectados debido a la gran digitalización de sus procesos bancarios. Existen numerosas formas de identificar la ciberdelincuencia de un país a otro, sin embargo, también existen factores comunes a nivel global, como el phishing, la fuga de datos y robos de identidad. A continuación, expondremos los niveles de seguridad por el entorno digital.

Según un informe publicado por SEON³ (2023), el CSIS⁴ emitió un advertencia en Enero 2023 en conjunto con tres autoridades estadounidenses de ciberseguridad -la CISA, la NSA (Agencia de Seguridad Nacional) y el MS-ISAC (Centro Multiestatal de Análisis e Intercambio de Información por el gran aumento de ciberataques, incluyendo phishing. También menciona, que en los diferentes países hay implementado productos antifraude para minimizar el riesgo, con el uso de enriquecimiento y monitoreo de datos, así como biometría o huellas digitales de navegadores y dispositivos con posibilidad de bloquear inicios de sesión sospechosos.

En México, por ejemplo, según NA-AT(2023) impulsan practicas muy similares a las que recomendamos en Argentina de cara a los usuarios, entre ellas destacamos el crear contraseñas seguras y cambiarlas con regularidad, habilitar la autenticación multifactor, utilizar tarjetas de débito y crédito segura y utilizar antivirus y firewall. Al mismo tiempo, tal como en Argentina tiene establecidas por los reguladores que aplican a todas las entidades financieras y deben implementarse sin excepción.

En Estados Unidos, según aconseja la agencia de seguridad de ciberseguridad e infraestructura (2023), se debe tener antivirus en todos los dispositivos que se utilicen, usar claves robustas y seguras, evitar abrir correos spam, chequear los sitios a los que se acceden, así como una vez que finaliza la operatoria realizar el deslogueo. También mencionan al igual que en la mayoría de los países, el uso de factores de autenticación múltiples y seteo de configuraciones de privacidad de los datos.

Por último, haciendo un relevamiento de Colombia, se pudo identificar que hacen las mismas recomendaciones que en los países ya mencionados. Según la editorial de WorldRemit (2023), se deben seleccionar nombres de usuario y contraseñas únicas en cada caso, así como acceder a las cuentas desde redes seguras. Remarcan el uso de antivirus, acceso a sitios seguros y múltiples factores de autenticación, así como también, la utilización de biometría y de activación de alertas para cualquier movimiento que se realicen en las cuentas. A diferencia de otros Mexico y Estados Unidos, en Colombia recomiendan la desactivación de bluetooth al igual que en Argentina.

³ Empresa antifraudes

⁴ El Centro de Estudios Estratégicos e Internacionales

4.4.1 Afectación de ciberataques en el mundo

A continuación, podremos visualizar una estadística provista por SEON, la cual se basa en los datos provistos por tres importantes autoridades de ciberseguridad, el Índice Nacional de Ciberseguridad (NCSI) (actualizado en tiempo real), el Índice Global de Ciberseguridad (GCI) (2020) y el Índice de Exposición a la Ciberseguridad (CEI) (2020), para identificar los países más afectados por la ciberseguridad.

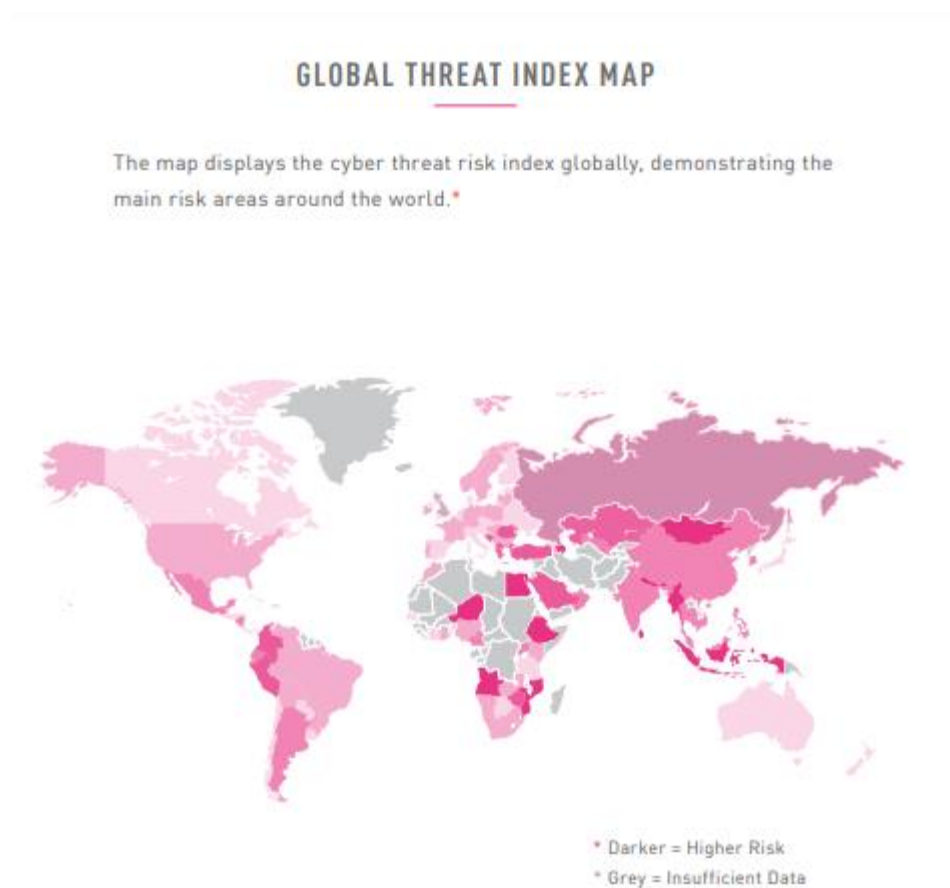
A continuación, se expondrán los 10 países más débiles en ciberseguridad de los 93 países analizados por SEON, quienes explican que “Estos países tienen una legislación muy débil en materia de ciberdelincuencia o incluso ninguna y, por lo tanto, son los que más riesgo corren a la hora de procesar transacciones sensibles” (SEON, 2023, p.1).

Figura 4

Los 10 países con mayor riesgo de ciberamenazas



Nota. El grafico representa los 10 países principales afectados por ciberamenazas. Tomado del informe global sobre ciberdelincuencia: ¿Qué países sufren mayor riesgo? presentado por SEON, 2023.

Figura 5*Mapa global de riesgo de ataque cibernético*

Nota. El gráfico muestra por un lado en rojo y morado los países del mundo con mayor riesgo de afectación por ciberataques y en gris los países sobre los cuales no se tiene

Tabla 2*Puntuación en ciberseguridad*

País	Índice Nacional de Ciberseguridad (NCSI)	Índice Global de Seguridad (GSI) 2020	Índice de Exposición a la Ciberseguridad (CEI) 2020	Puntuación de Ciberseguridad (media de NCSI, GCI y CEI)
1. Afganistán	11.69	5.20	0.00	5.63
2. Birmania	10.39	36.41	9.00	18.60
3. Namibia	15.58	11.47	32.10	19.72
4. Libia	10.39	28.78	20.70	19.96
5. Honduras	22.08	2.20	39.70	21.33
6. Camboya	15.58	19.12	29.70	21.47
7. Mongolia	18.18	26.20	26.20	23.53
8. Etiopía	32.47	27.74	13.40	24.54
9. Venezuela	28.57	27.06	19.30	24.98
10. Nicaragua	29.87	9.00	40.00	26.29

En el mismo informe se adjuntó la tabla de clasificación de los 93 de los países analizados (tabla completa adjunto en anexos.), en base a la cual se pudo construir la siguiente clasificación de América Latina.

Tabla 3*Escala de países de América Latina*

País	Índice Nacional de Ciberseguridad (NCSI)	Índice Global de Seguridad (GSI) 2020	Índice de Exposición a la Ciberseguridad (CEI) 2020*	Puntuación de Ciberseguridad (media de NCSI, GCI y CEI)
Uruguay	59.74	75.15	65.20	66.70
Brasil	51.95	96.60	45.90	64.82
Paraguay	63.64	57.09	58.60	59.78
Colombia	53.25	63.72	41.00	52.66
Perú	62.34	55.67	35.20	51.07
Venezuela	28.57	27.06	19.30	24.98

Nota. La puntuación mayor puntuación indica mayor nivel de ciberseguridad. La escala es de mayor a menor

4.5 Campañas de concientización al usuario.

Las campañas de concientización al usuario son un factor muy importante en la ciberseguridad, ya que es la herramienta que tienen las entidades para intentar educar y concientizar al usuario sobre los riesgos que trae la digitalización. “Una campaña de concientización es una acción estratégica para aumentar la visibilidad pública de una causa. Se debe explicar por qué la causa es importante, detallar informaciones claves sobre el tema y guiar cómo pueden participar los seguidores” (Red Alianza Latina, 2022, p.1).

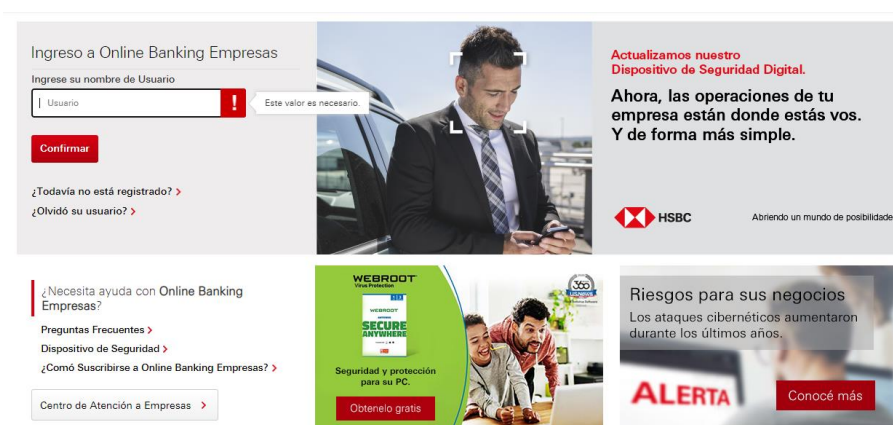
En 2022 se lanzó una campaña realizada por las entidades bancarias para prevenir a los usuarios en materia de seguridad, donde les brindaban diferentes tips a la hora de proteger sus datos personales y operar en las plataformas bancarias (Infobae, 2022).

Las diferentes entidades financieras generan contenido y campañas preventivas para los usuarios a través de sus plataformas, sitios públicos y redes sociales. Para generar estas campañas utilizan diferentes métodos con el fin de poder generar impacto en los clientes, entre ellos, podemos mencionar mails preventivos, banners con información o links a páginas de seguridad, alertas dentro de sus plataformas bancarias o *pop-up* con colores o imágenes sugerentes.

A continuación, se adjunta un ejemplo de banners de seguridad para prevención de usuario.

Figura 6

Sitio de empresas de HSBC



Nota. El grafico representa los banners con alertas y concientización al usuario. Tomado de la página de ingreso al homebanking, banca empresas, 2023, Banco HSBC.

5. Desarrollo Técnico

5.1 Introducción

En este capítulo, se detallan todas las variables y procedimientos que componen esta investigación. Se aborda cada aspecto relacionado con la metodología de investigación empleada, incluyendo los datos, las técnicas de recolección y los materiales utilizados. Finalmente, se describe con detalle el procesamiento de la información que condujo a los resultados, seguido de su análisis para derivar en las conclusiones.

5.2 Metodología de Investigación

En primer lugar, para explicar la metodología utilizada, señalo que “una investigación supone una cierta búsqueda bibliográfica, la obtención de datos de diverso tipo, y el procesamiento y análisis de los mismos” (Sabino, 1987, p.31). En el caso de este trabajo, podemos hacer una clasificación de carácter cualitativa basándonos en la comprensión profunda de fenómenos sociales, culturales o psicológicos, empleando ciertas técnicas de recolección de datos a través de técnicas como grupos focales y análisis de contenido; con el fin de obtener y descubrir patrones, significados y conceptos a partir de los datos. Según Hernández Sampieri y otros (2014) “el enfoque cualitativo utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación.” (p.7)

Los autores también argumentan que:

en la búsqueda cualitativa, en lugar de iniciar con una teoría y luego “voltear” al mundo empírico para confirmar si ésta es apoyada por los datos y resultados, el investigador comienza examinando los hechos en sí y en el proceso desarrolla una teoría coherente para representar lo que observa (Esterberg, 2002).

Dicho de otra forma, las investigaciones cualitativas se basan más en una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas). Van de lo particular a lo general.

Desde otro punto de vista, también se puede clasificar este trabajo como una investigación explicativa ya que, “Se enfocan explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variable” (Hernández Sampieri y otros, 2014, p. 98).

5.2.1 Recopilación y análisis de datos.

En esta apartado, se explicaran todos los datos que se utilizaron como variables de estudio para este trabajo de investigación, utilizando como premisa el alto impacto de los Malware en plataformas bancarias en Argentina.

En concordancia con las preguntas de investigación, se estableció como objetivo identificar las causas, efectos e impacto que pueden ocasionar las infecciones por Malware a los usuarios de las plataformas bancarias en Argentina. Se considero como unidad de estudio a los usuarios de diferentes rangos etarios y segmentos, que son quienes utilizan las plataformas bancarias, tanto para uso personal como laboral.

Es importante señalar que las computadoras pueden ser tanto personales como laborales, ya que el ingreso a estas plataformas es de dominio público y generalmente no está restringido; este es un punto de inflexión ya que en general, las computadoras laborales, suelen tener medidas de seguridad bastante más sofisticadas que las personales.

Tomando como base las preguntas de investigación y los objetivos del trabajo, se definieron las siguientes variables como marco de estudio:

1. Datos personales: nombre, edad, género y profesión.
2. Datos del equipo: uso, banco, cantidad de personas que la usan.
3. Antivirus: si tiene, cual, uso de aplicaciones riesgosas.
4. Conocimientos de Malware: que es, medidas de concientización, técnicas combinadas.
5. Conocimiento de afectaciones en el equipo: entendimiento de que puede hacer el malware si ingresa al equipo y que aplicaciones toma.

La versión final de la encuesta se generó con 10 preguntas, de las cuales 3 fueron para completar libres, 2 múltiple choice y 5 con respuesta dicotómica. Para asegurar la confiabilidad de la información obtenida, se envió el cuestionario a 40 personas, a través de la herramienta Survey Monkey. La encuesta se encontrará en la sección de anexos.

Por otro lado, se exponen y analizan datos y cantidad de ataques de malware detectados en los últimos 3 años en Argentina, comparados con los años previos al comienzo de la digitalización, como material complementario a la información obtenida del análisis de las encuestas realizadas.

5.3 Identificación y selección de casos de ciberataques malware.

En esta sección mencionaremos algunos de los Malwares que afectan a Argentina en la actualidad. Se mencionara el nombre, modus operandi y técnica con la cual se combina para poder ingresar al equipo. Principalmente, podemos hablar de lo siguientes Malware:

5.3.1 *Emotet*

Comenzaremos abordando al malware Emotet, un malware que al igual que en la mayoría de los casos detectados, se propaga a través de correos electrónicos spam o phishing con datos adjunto o enlaces infectados con código malicioso. Según Lizzette B. Pérez Arbesú, editora de la página TechTarget (2022), quien expuso lo publicado por Check Point Research⁵ (2022), está ubicado como uno de los malware más frecuentes en Junio 2022 en Argentina y su impacto es del 5,56%. Lo define como “ Un troyano avanzado, autopropagable y modular que en su día se utilizó como troyano bancario y que actualmente distribuye otro tipo de malware o campañas maliciosas”(Lizzette B. Pérez Arbesú, 2022, p.1).

5.3.2 *Mekotio*

Por otro lado, Mekotio es uno de los malware más actuales y con mayor afectación en las plataformas bancarias. Según el especialista en ciberseguridad, riesgo tecnológico y de negocios, Gabriel Zurdo comento en su entrevista (América TV, 2023, 1m40s) en estos casos el malware se instala a través de la técnica de phishing. Además, explica la casuística de la siguiente manera, el usuario afectado recibe un mail con el aviso de deuda de una multa o factura con un adjunto, el cual realmente es muy parecido a uno mail verídico con todos los detalles necesarios para crear la confusión. El usuario abre el adjunto para visualizar el detalle y con la apertura, se descarga un virus malicioso en la computadora llamado malware. A partir de ese momento, la PC queda infectada y el malware espera silencioso a que ingrese al homebanking para ejecutar lo llamado Keylogging y copiar todo lo que el usuario escribe para luego transaccionar en su nombre. A su

⁵ División de Inteligencia de Amenazas Check Point Software Technologies.

vez, el usuario visualiza una ventana emergente con una actualización de seguridad, la cual le inhabilita el control de la PC, dándole tiempo a Mekotio para que opere en nombre del usuario y sustraiga los fondos.

La agencia Télam⁶(2022) asegura que en los primeros 6 meses del 2022 se detectaron más 30 ataques de malware por minuto y 829 mil ataques de phishing, un aumento del 63% respecto del mismo período del 2021.

5.3.3 Qbot (Qakbot)

Qbot es un troyano que ingresa en la PC del usuario a través de correos electrónicos en spam simulando ser información importante con los recursos necesarios para que lo antivirus no detecten su existencia. Aparenta ser un archivo útil que no al abrirlo no genera ningún efecto inmediato, pero se ejecuta por detrás robando las credenciales bancarias y las pulsaciones de las teclas de los usuarios.

Según lo publicado en Tecnopymes(2023), Check Point Research catalogo a Qbot ⁷ como el troyano más predominante en los primeros 6 meses del año 2023, afectando al 10,27% de las empresas.

5.3.4 Conti

Conti es un ransomware que tuvo sus primeras apariciones en el año 2020 y desde entonces ha sido protagonista de múltiples ataques a organizaciones. “El ransomware Conti es la etapa final después de una intrusión exitosa en la red de las víctimas. La intrusión inicial podría realizarse mediante campañas de phishing, credenciales robadas o débiles para RDP o campañas de ingeniería social telefónicas”(Check Point Research, 2023, p.47).

5.3.5 Ataques de Ransomware a organizaciones

Según la Secretaría de Innovación Tecnológica del sector público, 2023, “El ransomware (conjunción de “ransom” -rescate- y software) es un programa malicioso, un malware que encripta determinados archivos de un dispositivo o sistema o el acceso a los mismos. El “secuestrador” de los datos solicita un “rescate”, un pago de criptomonedas, generalmente, para liberar la información”(pág.15).

Los fraudulentos empezaron a realizar copias de datos de manera remota antes de cifrarlos, para luego chantajear a la organización afectada, indicando que si no pagaban un rescate realizaban

⁶ La agencia de noticias más grande de Latinoamérica. Fundada en Argentina el 14 de abril de 1945

⁷ Troyano existente desde el año 2008.

la publicación en Internet de la información obtenida. Con la digitalización, hubo un aumento en los ataques aprovechando vulnerabilidades en los sistemas y comenzaron los ataques de "fuerza bruta" ⁸ contra los empleados de las organizaciones que accedían a las redes corporativas debido a la expansión del trabajo remoto o teletrabajo.

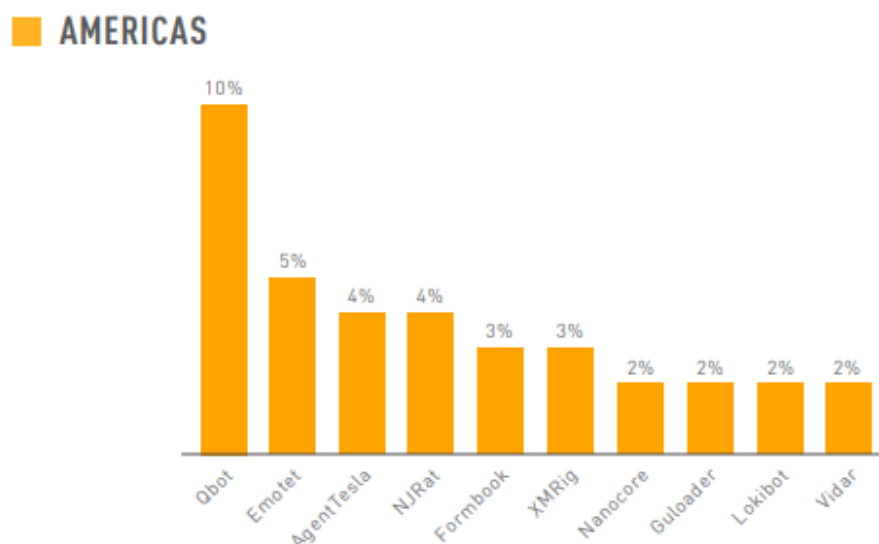
5.3.6. *Ramnit*

Ramnit se detectó por primera vez en 2013 y se lo conoce como un troyano bancario. Según Check Point Research (2023):

Roba la información de las sesiones web, dando a sus operadores la capacidad de robar las credenciales de la cuentas de todos los servicios utilizados por la víctima, incluyendo cuentas bancarias y de empresas y de redes sociales. El troyano utiliza tanto dominios codificados como dominios generado por un DGA (Algoritmo de Generación de Dominio) para contactar con el servidor C&C y descargar módulos adicionales.(p.49)

Figura 7

Familia de malware que más afectaron América.



⁸ Fuerza bruta: ataque cibernético donde el atacante intenta ingresar a un sistema informático probando diferentes combinaciones de caracteres hasta descubrir la contraseña deseada para ingresar a la cuenta de un usuario legítimo.

Nota. El gráfico muestra los porcentajes de afectación de cada malware en América.

Tomado del informe de Check Point Research, 2023, Mid-Year Cybersecurity report.

6. Resultados

6.1 Análisis de los resultados obtenidos.

En este capítulo se presentan los resultados obtenidos luego de una exhaustiva investigación, en el área de seguridad del usuario que utiliza las plataformas bancarias con respecto al aumento de los ciberataques de la mano de la digitalización. Durante el curso de esta investigación, hemos analizado y recopilado datos significativos relacionados con los ciberataques por malware y el impacto en el usuario de las plataformas bancarias, con el objetivo de arrojar luz sobre las posibles mejores y mitigantes para reducir el impacto actual.

Los resultados que se presentarán en las siguientes secciones ofrecen una visión detallada de los hallazgos y conclusiones que surgieron de este proceso. Estos resultados proporcionarán una comprensión más profunda de los ciberataques por malware y servirán como base para futuros análisis, decisiones y recomendaciones en el ámbito financiero.

6.1.1 Resultados obtenidos

En esta sección, presentaremos de manera detallada los datos y análisis resultantes de la encuesta realizada a una muestra representativa, con el objetivo de comprender cuan interiorizado están los usuarios en temas de digitalización y seguridad. Los resultados de esta encuesta proporcionan una visión valiosa sobre la temática de la investigación y ofrecen datos claves que puede ser utilizados para la toma de decisiones y/o mejoras en los procesos.

Muestra : 136 encuestas. Preguntas adjuntas en anexo.

Edad: muestra etaria entre 18 años a 85.

Para realizar la encuesta, se utilizó un enfoque de muestreo aleatorio simple. Se seleccionaron aleatoriamente un número de 136 personas de diferentes edades y condiciones para obtener un muestreo amplio y variado. Para garantizar la representatividad de la muestra se identificaron diversos universos a encuestar, con el fin de obtener una muestra real, identificando personas de diferentes rangos etarios y a su vez, dentro de un mismo rango etario con diferentes profesiones o situaciones socioeconómicas para participar en la encuesta logrando diversidad de población

elegida. Se aplicó un cuestionario estructurado que abarcaba temas como digitalización, hábitos, preferencias y conocimiento de la temática abordada.

La encuesta fue creada en una página llamada Survey Monkey,⁹ la cual no solo permite generar la encuesta, sino que también recopila las respuestas, permitiendo generar un análisis de los resultados. El sitio permite generar un link con la encuesta para luego compartirlo rápidamente por mail y/o WhatsApp. Las respuestas se almacenan de manera electrónica dentro del sitio para su posterior visualización y análisis.

Análisis inicial:

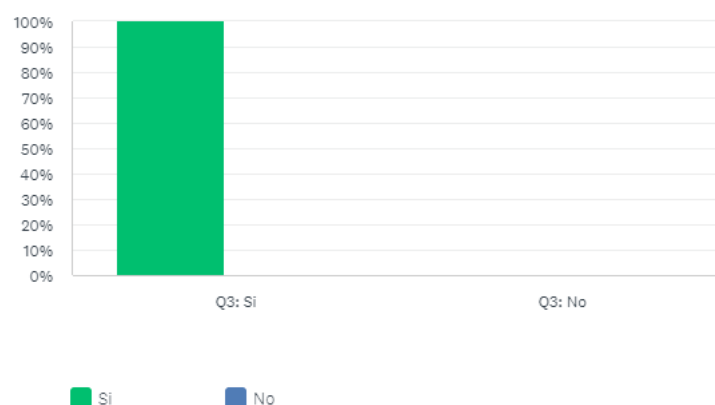
Podemos ver que el 100% de los usuarios administran sus cuentas por plataformas digitales, un 53% de ellos las utilizan hace menos de 5 años, pero solo el 48% de ellos utilizan un antivirus en sus dispositivos:

Figura 8

Respuestas pregunta 3

¿Usas plataformas bancarias para administrar tus cuentas?

Respondidas: 136 Omitidas: 0



Nota. El gráfico muestra las respuestas obtenidas de la encuesta en cuanto al uso de las plataformas bancarias. De autoría propia, 2023, Survey Monkey.

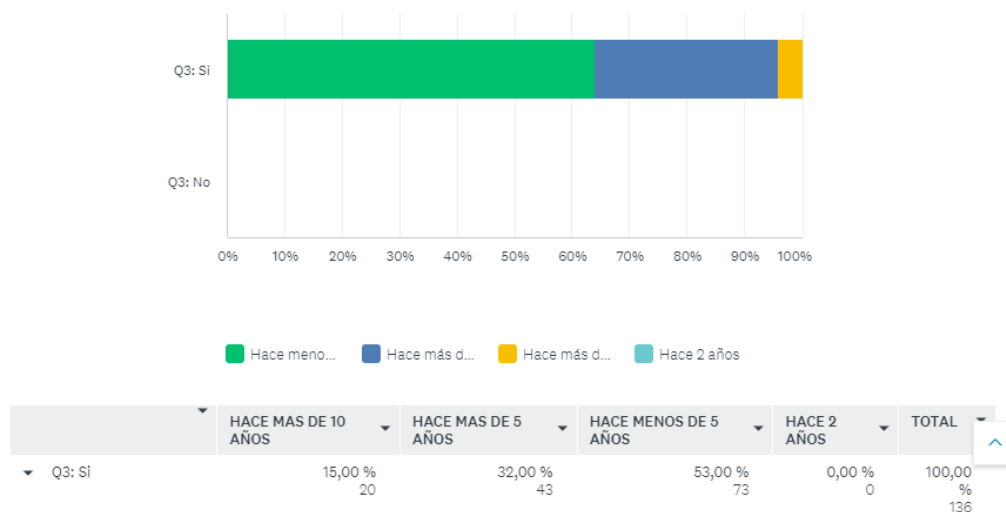
⁹ Empresa estadounidense que permite generar encuestas.

Figura 9

Respuestas pregunta 4

Si la respuesta anterior fue si, ¿Hace cuantos años?

Respondidas: 136 Omitidas: 0



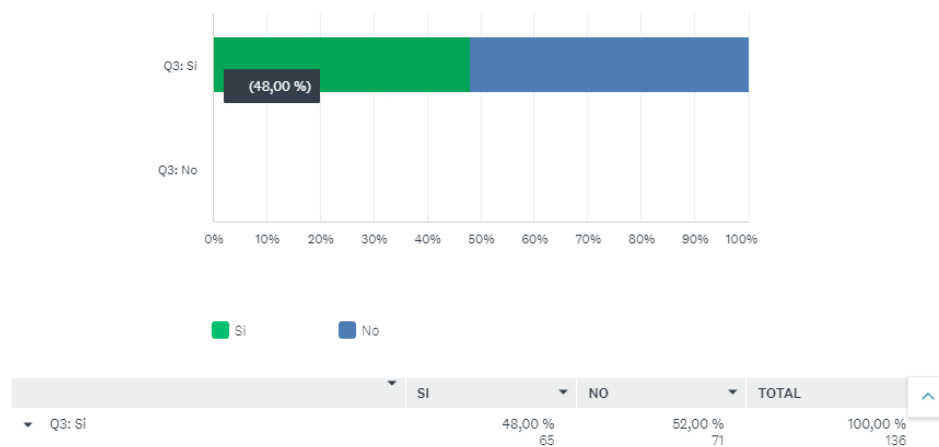
Nota. El grafico muestra los porcentajes obtenidos en la encuesta sobre antigüedad de uso de las plataformas bancarias. De autoría propia, 2023, Survey Monkey.

Figura 10

Respuestas pregunta 5

¿Tiene antivirus?

Respondidas: 136 Omitidas: 0



Nota. El grafico muestra las respuestas obtenidas en cuento al uso de antivirus por los usuarios encuestados. De autoría propia, 2023, Survey Monkey.

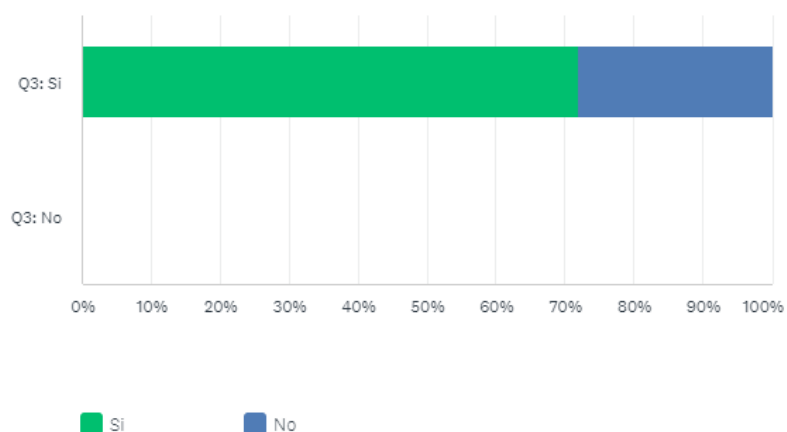
Analizando si las personas que utilizan plataformas bancarias tienen algún tienen conocimientos sobre lo que es un malware o phishing, pudimos determinar que el 72% tienen conocimientos de estas casuísticas, pero solo el 64% toma recaudos sobre los mails que abren o link en los que ingresan.

Figura 11

Respuestas pregunta 6

¿ Sabes que es el phishing o que es malware?

Respondidas: 136 Omitidas: 0

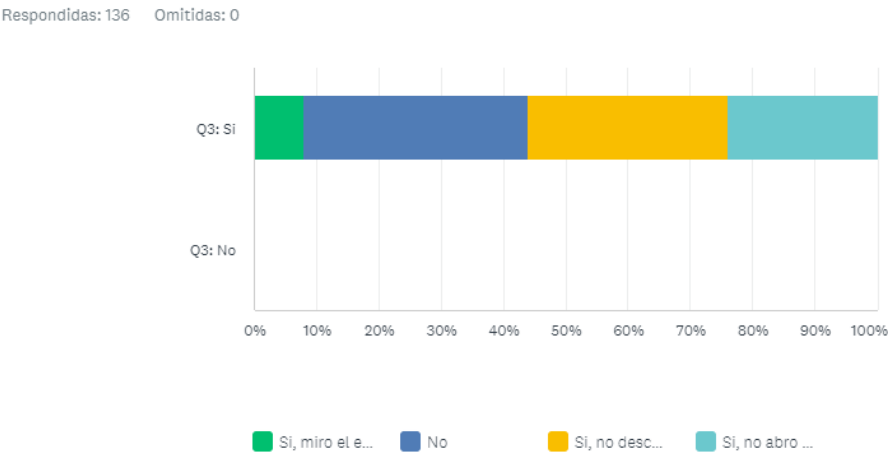


Nota. El grafico muestra las respuestas obtenidas sobre el conocimiento de los conceptos de phishing y malware. De autoría propia, 2023, Survey Monkey.

Figura 12

Respuestas pregunta 8

¿ Haces validaciones antes de abrir un mail o descargar un adjunto? ¿Cuales?



Nota. El grafico muestra las respuestas obtenidas en cuanto a la precaución de los usuario en la operatoria diaria de sus cuentas. De autoría propia, 2023, Survey Monkey.

Contamos con la siguiente premisa:

Tabla 4

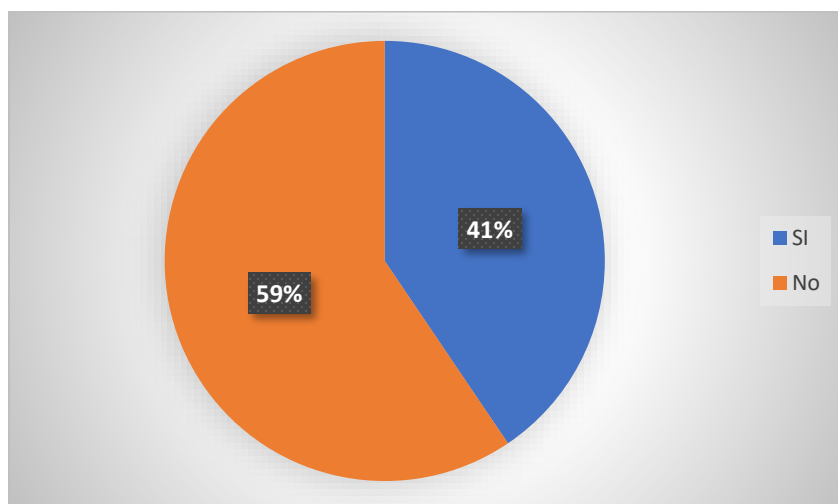
Encabezado de la encuesta

Total de respuestas	Índice de encuestas completadas	Tiempo utilizado normalmente	Preguntas que más omitieron
136	100%	1m:36s	Q10 - Si la respuesta anterior fue si, describilo. Omitido:76

Si bien la estadística menciona que la pregunta 10 fue la más omitida, está en línea con la pregunta 9 donde se encuesta a los usuarios sobre si habían sufrido un ataque cibernético o si sabían de alguien que lo haya sufrido. Si bien el 100% de los usuarios respondieron esa pregunta con la siguiente estadística:

Figura 13

Respuestas de la pregunta 9



Nota. El grafico muestra el porcentaje de usuarios que conocen a alguien que sufrió un ataque cibernético. De autoría propia, 2023, Survey Monkey.

Hay un 55.8% que no contestaron la pregunta 10, la cual apuntaba a comentar el ciberataque o casuística que sufrieron o les contaron, debido a que su repuesta anterior fue NO.

En cuanto a los 60 encuestados que respondieron la pregunta 10 sobre la casuística sufrida se obtuvieron las diferentes casuísticas y las agrupe en los siguientes grupos de manera genérica para clasificarla por tipo de ciberataque:

Tabla 5*Clasificación de casuísticas detectada*

Casuística detectada	Clasificación		
	Phishing	Malware	Ingeniería Social
Ingreso a paginas duplicadas o falsas.		x	
Ingreso a links maliciosos	x		
Compartir códigos de token por error.			x
Compartir datos de las tarjetas.			x
Instalación de virus.	x	x	
Información que no aplica a la respuesta.			
Toma de control del homebanking.	x	x	x
Mails maliciosos.	x		
Robo de datos y generación de compras varias.		x	x
Hackeo de WhatsApp.			x

Por ende, podemos concluir que en la mayoría de los casos se combinan las técnicas de ataques para lograr una ejecución exitosa.

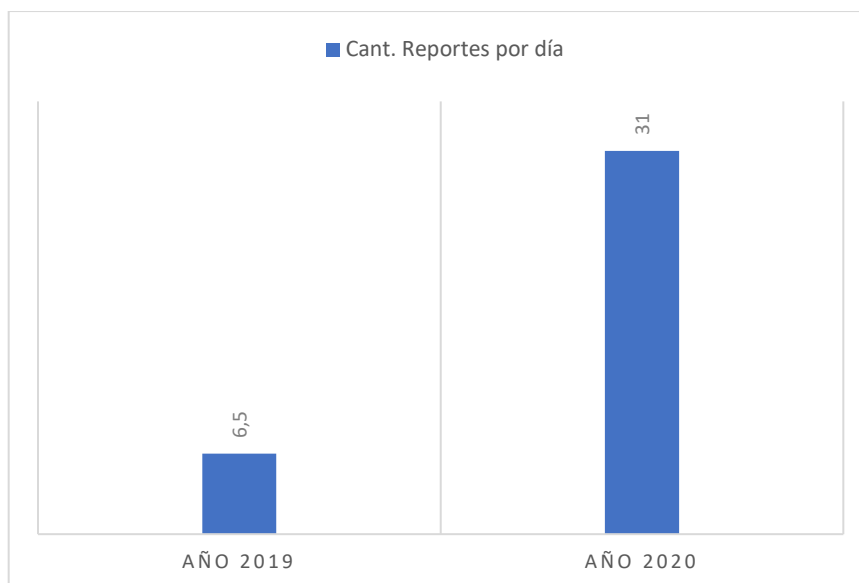
6.1.2 Datos reales del impacto de la digitalización

La digitalización comenzó a tomar una gran relevancia en el año 2020 con la llegada de la pandemia, a raíz de esto, la gente comenzó a utilizar las plataformas bancarias de manera diaria para todas sus operatorias. Como consecuencia de esta digitalización se vio un gran aumento en los ciberataques en Argentina, donde según la UEFI (2021), en tan solo un año aumento la cantidad de ataques en un 381%.

A continuación, adjunto diferentes gráficos que demuestran el crecimiento de los fraudes por la digitalización relevado por la UEFI (2021) en su informe, Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020

Figura 14

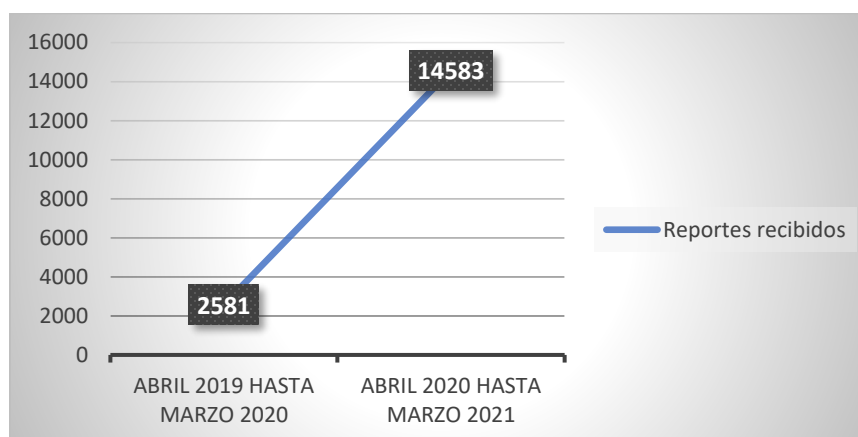
Ataques reportados por día



Nota. En el grafico se representa el aumento de reportes diarios de ataques cibernéticos que se recibieron en los periodos especificados. Tomado de Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020, UEFI, 2021.

Si tomamos en cuenta el año previo a la pandemia los meses de abril de 2019 y marzo de 2020 en comparación con los meses de abril de 2020 y marzo de 2021 el aumento de reportes recibidos es del 465%.

Figura 15

Reportes recibidos

Nota. En el grafico se representa el aumento de reportes recibidos de ataques cibernéticos que se recibieron en comparación de Abril 2019 a Marzo 2020 vs Abril 2020 a Marzo 2021. Tomado de *Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020*, UEFI, 2021.

Tabla 6

Cantidad de fraudes detectado.

Año/ Rubro	Fraudes digitales
12 meses previo a la pandemia	16
12 primeros meses de pandemia	1064
Aumento Porcentual	6550%

Nota: Refleja el acceso indebido a plataformas de banca en línea o homebanking.

ITWARE Latam (2023) publicó un artículo acerca del gran impacto de los ciberataques en Argentina, para ellos se basó en el reporte publicado por Check Point Research del primer trimestre del 2023 donde aseguraron que hubo un incremento en ataques semanales del 22% en comparación

al mismo periodo del año anterior y el numero semanal promedio de ciberataques aumento hasta 2.052.

En el informe se detallan los porcentajes de aumento de ciberataque por rubro, y podemos ver que en el ámbito financiero/ bancario se detecta una suba del 9% con respecto al mismo periodo de 2022.

Figura 16

Incremento de ciberataques por segmento



Nota. En el grafico se representa el aumento de ciberataques en Latinoamérica por cada segmento afectado y el porcentaje de crecimiento. Tomado de *Reporte del primer trimestre del año 2023, Check Point Research, 2023, ITWARE Latam.*

Por otro lado, y de acuerdo al reporte de mitad de año de Check Point Research (adjunto en anexos), según Tecnopymes(2023), se revela un 8% de aumento más en los ataques semanales, tomando este, como uno de los incrementos más significativos en los últimos dos años, realizando el énfasis en que la causa es la digitalización combinada con el uso de IA. El informe también revela como aumentaron en esta primera mitad de año los ataques por Ransomware, aumentando en un 21% con respecto al mes anterior.

. “La probabilidad y efectividad de los ciberataques puede reducirse con medidas proactivas como campañas de concientización y tecnologías de seguridad adecuadas”(Alejandro Botter, gerente de ingeniería de Check Point para el sur de Latinoamérica, 2023).

6.2 Medidas de seguridad

Basándose en los datos recolectados y los resultados de las encuestas, y con el objetivo de contribuir a la mitigación de los ciberataques, se propone una estrategia integral que incluye posibles mejoras para reducir el impacto directo en los usuarios y minimizar su exposición a estos ataques. Se proponen cambios a nivel nacional y a nivel de entidad.

Por un lado, es fundamental comenzar a contar con una base de usuarios y status, donde se contenga la información de todas las personas bancarizadas. Se podría generar una base de usuarios en alguna de las cámaras compensadoras como por ej.: Coelsa¹⁰, donde se pueda registrar el status de cada ID bancario (clave de identificación del cliente como DNI o CUIL/CUIT), para luego poder ser consultado. Cuando un banco recibe la denuncia de un cliente sobre un fraude o intento de fraude a un ID lo informan en esta base de manera online, para que todos los bancos puedan saber que puede estar siendo usurpado por un ciberdelincuente. A raíz de esa información las entidades pueden implementar diferentes validaciones adicionales sobre ese usuario para asegurar un ingreso seguro.

La base es única y está disponible para todas las entidades, permitiendo una constante retroalimentación y comunicación entre todos los bancos para ofrecer una seguridad integral en la operatoria de sus plataformas.

Por otro lado, cada cliente debe tener una huella única, muchas entidades utilizan sistemas de monitoreo en los cuales guardan la información de los clientes generando un *fingerprint*¹¹ del mismo, si bien es un control eficiente para esa entidad, pierde su eficacia cuando hablamos de soluciones integrales. Lo que se plantea, es generar una base única, que todas las entidades puedan nutrir y consultar sobre la huella del cliente, como, por ejemplo, que dispositivo usa, que versión, con qué frecuencia, IP, factor de validación, etc. De esta manera logramos un perfil Integral que nos permite alertar a todas las entidades frente a una sospecha de ciberataque.

Por último, debemos tener la posibilidad de implementar la autorización de transacciones con control cruzado de canales: según el relevamiento se puede identificar que la mayoría de los ataques ingresan por medio de un phishing que infecta el computador; por lo tanto, si la confirmación de la operación se ejecuta por otro canal diferente al infectado, se reduciría la

¹⁰ Coelsa: Cámara compensadora bancaria.

¹¹ Fingerprint: huella digital de comportamiento del cliente

cantidad de casos de éxito. Esta solución debe incluir diferentes tipos de patrones y segmentación de acuerdo al uso de la plataforma.

7. Conclusiones

Luego del análisis realizado en el presente trabajo de investigación podemos concluir que se identificaron ciertos comportamientos, tendencias y desafíos claves en el entorno bancario vs la ciberseguridad. Los casos analizados han revelado la necesidad imperativa de que los bancos reorienten su enfoque central hacia la seguridad de los usuarios, priorizándola sobre las políticas comerciales. Este cambio implica un crecimiento continuo en materia de ciberseguridad para fortalecer la confianza de los usuarios, la cual depende de la robustez de las plataformas. Se observa un movimiento hacia la conceptualización de las plataformas digitales bancarias no solo como transaccionales, sino también como relacionales.

Por otro lado, se demuestra que las implementaciones de seguridad realizadas por las entidades bancarias hasta el momento han sido mejoras aisladas o protocolos diferentes, los cuales han demostrado ser ineficaces en el corto y mediano plazo. A pesar de la participación gubernamental en la publicación y sanción de normas que regulan la digitalización bancaria, como así también los requisitos mínimos de seguridad en la infraestructura de las plataformas, sin embargo, siguen siendo insuficientes para el creciente contexto actual en materia de seguridad digital bancaria.

La inversión en tecnologías de seguridad avanzadas emerge como un aspecto central y vital para el futuro inmediato, obligando a las entidades bancarias a desarrollar sistemas lo suficientemente robustos para detectar diversas intrusiones, y lo bastante flexibles y escalables para adaptarse a las evoluciones del mercado. No obstante, persiste una resistencia significativa por parte de los bancos hacia la inversión en temas y sistemas de seguridad, adoptando una postura reactiva frente a los fraudes en lugar de una proactiva.

En concordancia con los datos recolectados, se observa un crecimiento alarmante de los ataques por malware en el ámbito financiero, reflejando un incremento constante en la cantidad, calidad y sofisticación de estos ataques mes a mes. Estas estadísticas se con las encuestas que revelan el bajo nivel de conocimiento de los usuarios sobre estas amenazas, subrayando la urgente necesidad de abordar el problema de manera efectiva.

Se identificó un rol notablemente pasivo por parte de los usuarios, cuya falta de información y educación en seguridad digital contribuye en gran medida a los ciberataques, especialmente aquellos vinculados al malware, phishing y otras tácticas de ingeniería social dirigidas directamente a los usuarios de plataformas digitales. Estas amenazas en constante

evolución requieren una mayor concienciación por parte de los usuarios sobre las prácticas de seguridad. Aunque se observa un aumento en las campañas de concientización digital, aún no se ha alcanzado una alta tasa de eficacia.

La creciente y rápida digitalización de los bancos ha expuesto una brecha significativa entre los beneficios de digitalizar las plataformas y la necesidad imperiosa de una seguridad integral para asegurar el éxito funcional en el entorno digital actual.

8. Líneas Futuras De Investigación

El uso de inteligencia artificial, machine learning y análisis de comportamiento juega un papel crucial en la identificación y detección de nuevas variantes de malware en el entorno digital actual. Estas tecnologías avanzadas permiten a las organizaciones de seguridad cibernética anticiparse y responder de manera proactiva a las amenazas emergentes, que están en constante evolución y se vuelven cada vez más sofisticadas.

Cuando se combinan estas técnicas, se crea un enfoque poderoso para la detección de nuevas variantes de malware. La IA y el machine learning pueden analizar grandes conjuntos de datos y aprender a reconocer características y patrones asociados al malware. A medida que se encuentran nuevas amenazas, estos sistemas pueden adaptarse y mejorar su capacidad de detección sin intervención humana constante.

Además, el análisis de comportamiento permite detectar el malware según su actividad, incluso si las características específicas del malware son desconocidas. Esto es fundamental porque los atacantes desarrollan constantemente nuevas variantes de malware para evadir la detección tradicional basada en firmas.

9. Referencias

Accion.point. (17 de febrero de 2023). *Plataformas bancarias centradas en el cliente: qué diferencial aportan*. Action Point. <https://accionpoint.com/blog/plataformas-bancarias-centradas-en-el-cliente-que-diferencial-aportan/>

Acosta, C. (16 de Junio de 2022). *Los principales riesgos de la digitalización bancaria*. Debmedia. <https://debmedia.com/blog/principales-riesgos-de-la-digitalizacion-bancaria>

Amaiquema Chuquiana Evelyn Maoli. (2023). *Análisis del ataque del modelo phishing en los sistemas informáticos bancarios*.
<http://dspace.utb.edu.ec/bitstream/handle/49000/14773/E-UTB-FAFI-SIST-000437.pdf?sequence=1&isAllowed=y>

América TV. (13 de Abril de 2023). *Alerta por Mekotio, un virus bancario*. YouTube. <https://www.youtube.com/watch?v=iX0dtIf0prM>

AVAST. (2023). *Seguridad*. <https://www.avast.com/es-es/c-category-security>

Banco Santander. (2024). *¿Qué es y para qué sirve el Home Banking?*
<https://santanderpost.com.ar/articulo/que-es-y-para-que-sirve-el-home-banking/>

Basque Cybersecurity Centre. (2021). *Mekotio*.
<https://www.ciberseguridad.eus/sites/default/files/2022-04/bcsc-malware-mekotio-tlpwhite816.pdf>

BCRA. (2016). *Comunicación A “6017”*.
<https://www.bcra.gob.ar/pdfs/comytexord/A6017.pdf>

BCRA. (2023). *Comunicación A “7783”*.
<https://www.bcra.gob.ar/pdfs/comytexord/A7783.pdf>

BCRA. (2023). *Comunicación A “7777”*.
<https://www.bcra.gob.ar/Pdfs/comytexord/A7777.pdf>

BCRA. (2016). *Comunicación A “7773”*.
<https://www.bcra.gob.ar/pdfs/comytexord/A7773.pdf>

BCRA. (2016). *Comunicación A “6656”*.
<https://www.bcra.gob.ar/Pdfs/comytexord/A6656.pdf>

BCRA. (2016). *Comunicación A “6480”*.
<https://www.bcra.gob.ar/Pdfs/comytexord/A6480.pdf>

Belcic, I. (23 de Febrero de 2023). *Guía esencial del phishing: cómo funciona y cómo defenderse*. <https://www.avast.com/es-es/c-phishing>

Belcic, I. (25 de Junio de 2023). *¿Qué es el malware y cómo protegerse de los ataques?* <https://www.avast.com/es-es/c-malware>

Cámara Argentina de Comercio y Servicios. (2020). *Ciberseguridad: la importancia de estar protegidos*. https://dep.cac.com.ar/ola_digital_noticia/ciberseguridad_la_importancia_de_estar_protegidos_42

Cámara Valencia. (2016). *Qué es un ciberataque y qué tipos existen*. <https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/>

Check Point Research. (2023). *Reporte de ciberseguridad mitas de año*. <https://pages.checkpoint.com/2023-mid-year-cyber-security-report.html>

CISCO. (2023). *Seguridad*. https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html#~temas-relacionados

COFEDEC Argentina Gobierno (2022). *Ciberdelitos y Estafas Digitales Consejo Federal del Consumo*. https://www.argentina.gob.ar/sites/default/files/cuadernillo_2_-_cofedec1.pdf

Cloud.gal. (2023). *La importancia de las copias de seguridad en la nube para mitigar ciberataques*. <https://www.cloud.gal/por-que-cloud-gal/>

Cybersecurity & infrastructure security agency. (2023). *SHIELDS UP!* <https://www.cisa.gov/shields-up>

Cyberzaintza. (2023). *Malware bancario*. <https://www.ciberseguridad.eus/ciberpedia/fraudes/malware-bancario>

Dan Shoemaker y Wm. Arthur Conklin. (2011). *"Cybersecurity: The Essential Body of Knowledge"*

Díaz, F. (27 de Marzo de 2018). *Arrestado el líder detrás de Cobalt y Carbanak. Una al día*. <https://unaaldia.hispasec.com/2018/03/arrestado-el-lider-detras-de-cobalt-y-carbanak.html>

DigiALERT. (23 de Marzo de 2023). *Case Study on Bangladesh Banking Heist*. LinkedIn. <https://www.linkedin.com/pulse/case-study-bangladesh-banking-heist-digialert/>

Dirección Nacional de ciberseguridad. (2021). *Botnets*. https://www.argentina.gob.ar/sites/default/files/2021/07/informe_botnets_-_julio_2021.pdf

Dzigciot, JA. (27 de Noviembre 2022). *La Transformación Digital y los Riesgos*. LinkedIn. <https://www.linkedin.com/pulse/la-transformaci%C3%B3n-digital-y-los-riesgos-adolfo-jos%C3%A9-dzigciot/?originalSubdomain=es>

ESET. (2023). *Mekotio: un conocido troyano bancario que sigue activo en América Latina*. <https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/mekotio-un-conocido-troyano-bancario-que-sigue-activo-en-america-latina0/>

Faster Capital. (2023). *Evolución del malware ascenso y caída de los troyanos bancarios*. <https://fastercapital.com/es/contenido/Evolucion-del-malware--ascenso-y-caida-de-los-troyanos-bancarios.html>

Forbes AR. (2022). *Banca y digital, una transformación real*. <https://www.forbesargentina.com/columnistas/banca-digital-una-transformacion-real-n19739>

Funcas. (2020). De la banca digital a las plataformas bancarias digitales(DBP). <https://www.funcas.es/odf/de-la-banca-digital-a-las-plataformas-bancarias-digitales-dbp/>

Gobierno Nacional Argentina. (2021). *Ley de Entidades Financieras-Ley 21.526* <https://www.argentina.gob.ar/normativa/nacional/ley-21526-16071/actualizacion>

Gobierno Nacional Argentina.(2008). *Ley de Delitos Informáticos- Ley 26.388*. <https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto>

Gobierno Nacional Argentina.(2000). *Ley de Protección de Datos Personales-Ley 25.326*. <https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790>

Gobierno Nacional Argentina.(2019). *Ley de Firma Digital- Ley 25.506*. <https://www.boletinoficial.gob.ar/detalleAviso/primera/203048/20190312>

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación (6 ed.)*. México: MCGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

HSBC (2023). *Homebanking empresas*. <https://www.obempresas.hsbc.com.ar/bib/login>

IBM. (2023). *¿Qué es un ciberataque?* <https://www.ibm.com/es-es/topics/cyber-attack>

IBM. (2023). *Ciberseguridad*. <https://www.ibm.com/es-es/topics/cybersecurity>

INCIBE. Instituto Nacional de Ciberseguridad de España. (2021). *Estudio del análisis de Mekotio*. https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_mekotio_2021_v1.pdf

Infobae. (11 de Febrero del 2022). *Bancos públicos y privados lanzaron una campaña para prevenir estafas digitales: 12 tips para proteger los datos personales*. Recuperado el 27 de Octubre del 2023 de <https://www.infobae.com/economia/2022/02/11/bancos-publicos-y-privados-lanzaron-una-campana-para-prevenir-estafas-digitales-12-tips-para-proteger-los-datos-personales/>

Infosecurity México. (2023). Ciberseguridad. <https://www.infosecuritymexico.com/es/ciberseguridad>.

ITWARE Latam. (2023). *Argentina lidera el ranking regional de ciberataques*. <https://www.itwarelatam.com/2023/05/02/argentina-lidera-el-ranking-regional-de-ciberataques/>

José Luis Portocarrero. (2023). *Banking as a Service (BaaS): Innovación y oportunidades en la era digital*. <https://www.linkedin.com/pulse/banking-service-baas-innovaci%C3%B3n-y-oportunidades-en-la-portocarrero/?originalSubdomain=es>

Lisa Institute. (2019). Lista de 45 consejos de seguridad bancaria: ¿Cómo mantener mis cuentas bancarias seguras? <https://www.lisainstitute.com/blogs/blog/consejos-seguridad-bancaria>

McAfee. 2023. *¿Qué es malware?* <https://www.mcafee.com/es-ar/antivirus/malware.html>

Mendoza, M. (02 de Junio de 2023). *Mekotio: un conocido troyano bancario que sigue activo en América Latina*. We live Security. <https://www.welivesecurity.com/la-es/2023/06/02/mekotio-conocido-troyano-bancario-sigue-activo-america-latina/>

Mónica Tilves. (2021). *A fondo: Emotet, el final de un 'malware' endiablado*. <https://www.silicon.es/a-fondo-emotet-el-final-de-un-malware-endiablado-2431302>

NA-AT. (2023). *Descifrando el concepto de seguridad bancaria y financiera: Normas y Prácticas* *Clave*. <https://blog.na-at.com/es/descifrando-el-concepto-de-seguridad-bancaria-y-financiera-normas-y-practicas-clave#:~:text=A%20grandes%20rasgos%2C%20la%20seguridad,el%20robo%20o%20el%20ciberataque>.

NTT DATA. (2023). *Tipos de ciberataques y cómo hacerles frente*. <https://es.nttdata.com/insights/blog/tipos-de-ciberataques-y-como-hacerles-frente>

Olivera, M. (10 de Noviembre de 2023). *La evolución de la ingeniería social en la ciberseguridad*. LinkedIn. https://www.linkedin.com/pulse/la-evoluci%C3%B3n-de-ingenier%C3%ADa-social-en-ciberseguridad-silent4business-knaoe/?trk=public_post_main-feed-card_feed-article-content

Página 12. (13 de abril de 2023). *Mekotio, el nuevo virus troyano que ya lleva robado 61 millones de pesos*. <https://www.pagina12.com.ar/540315-mekotio-el-nuevo-virus-troyano-que-ya-lleva-robado-61-millon>

Pérez Arbesú, L. (22 de Julio de 2023). *Emotet lideró las infecciones de malware en Argentina durante junio*. TechTarget. <https://www.computerweekly.com/es/cronica/Emotet-lidero-las-infecciones-de-malware-en-Argentina-durante-junio>

P.W. Singer y Allan Friedman. (2014). "*Cybersecurity and Cyberwar: What Everyone Needs to Know*."

Red Alianza Latina. (2021). *Manual práctico sobre campañas de concientización*. <https://redalianzalatina.org/es/biblioteca-es/manual-practico-sobre-campanas-de-concientizacion/>

Secretaria de Innovación Tecnológica del Sector Publico. (2022). *Delitos informáticos en Argentina*. https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf

Seguin, P., Latto, N. (12 de Abril de 2023). *La guía esencial sobre el ransomware*. <https://www.avast.com/es-es/c-what-is-ransomware>

SEON. (2023). *Informe global sobre ciberdelincuencia: ¿Qué países corren mayor riesgo?* <https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/>

Tecnopymes. (2023). *Check Point revela un aumento del 20% en los ciberataques de Argentina*. <https://tecnopymes.com.ar/2023/09/11/check-point-revela-un-aumento-del-20-en-los-ciberataques-de-argentina/>

Tecnopymes. (2023). *Qbot es el malware más prevalente en 2023*. https://tecnopymes.com.ar/2023/08/17/qbot-es-el-malware-mas-prevalente-en-2023/?utm_source=rss&utm_medium=rss&utm_campaign=qbot-es-el-malware-mas-prevalente-en-2023

UEFI. (2021). *Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020*. https://www.mpf.gob.ar/ufeci/files/2021/09/UFECI_informe-pandemia.pdf

Veritas Technologies. (2022). *Software malicioso: ¿Qué es y cómo protegerse?* <https://www.veritas.com/es/es/information-center/malware>

WorldRemit. (2023). *Seguridad financiera en Colombia: ¿cómo proteger tus cuentas?*
<https://www.worldremit.com/es/blog/finance/seguridad-financiera-en-colombia-como-proteger-tus-cuentas>