UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

ANÁLISIS DE LOS ATAQUES CIBERNÉTICOS EN LA BANCA ECUATORIANA: MAPEO SISTEMÁTICO

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

AUTORES: Monar Montes David Israel.

Vergara Aviles Alan Joshue.

TUTOR: Nelson Salomón Mora Saltos, Msig

Guayaquil – Ecuador

2023

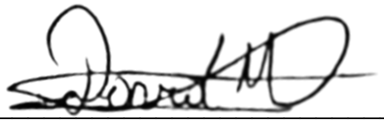
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, David Israel Monar Montes, con documento de identificación N° 0921891107, y Alan Joshue Vergara Aviles, con documento de identificación N° 0956549430 manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 16 de marzo del año 2023

Atentamente,



David Israel Monar Montes
0921891107

Alan Joshue Vergara Aviles
0956549430

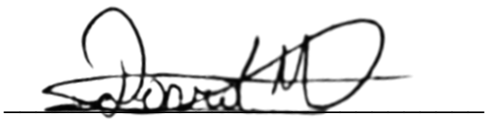
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, David Israel Monar Montes, con documento de identificación N° 0921891107, y Alan Joshue Vergara Avilés, con documento de identificación N° 0956549430, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Artículo Académico: "ANÁLISIS DE LOS ATAQUES CIBERNÉTICOS EN LA BANCA ECUATORIANA: MAPEO SISTEMÁTICO", el cual ha sido desarrollado para optar por el título de: Ingeniero en la Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

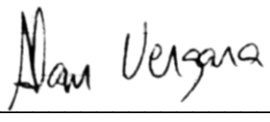
En concordancia con lo manifestado, suscribimos este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 16 de marzo del año 2023

Atentamente,



David Israel Monar Montes
0921891107



Alan Joshue Vergara Aviles
0956549430

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Nelson Salomón Mora Saltos, Msig con documento de identificación N° 0909257800, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANÁLISIS DE LOS ATEQUES CIBERNÉTICOS EN LA BANCA ECUATORIANA: MAPEO SISTEMÁTICO, realizado por David Israel Monar Montes, con documento de identificación N° 0921891107, y Alan Joshue Vergara Avilés, con documento de identificación N° 0956549430, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 16 de marzo del año 2023

Atentamente,

Nelson Salomón Mora Saltos, Msig.
0909257800

DEDICATORIA

Este trabajo va dedicado a mis padres, debido al esfuerzo y apoyo que me brindaron durante toda esta etapa de mi vida, a mi hijo ya que es el motor que me impulsa a cumplir mis objetivos que se me presentan en el diario vivir, a mi hermana Gabriela por los consejos que me supo brindar cuando más lo necesitaba.

David Israel Monar Montes

Dedico este trabajo a mi padre el Ab John Vergara, a mi madre Jacqueline Avilés, a mis hermanos y en el especial a mi hermano mayor Jonathan que ya no está conmigo en estos momentos, mi sobrino Joaquín y a toda mi familia que estimo mucho.

Alan Joshue Vergara Aviles

AGRADECIMIENTO

Agradezco a la Universidad por acogerme con los brazos abiertos, a mis maestros que siempre fueron un pilar fundamental para forjarme como profesional, a mi familia por todo el sacrificio que realizaron para poder cumplir mis objetivos, y a nuestro señor Dios por otorgarme la sabiduría necesaria para poder cumplir con los propósitos que me he propuesto.

David Israel Monar Montes

Agradezco a Dios en primer lugar por dame esta oportunidad de culminar mis estudios, a mis padres que siempre me apoyaron económica y anímicamente para nunca rendirme, a mis profesores que siempre nos motivaron y mis amigos de los primeros semestres hasta ahora.

Alan Joshue Vergara Aviles

RESUMEN

Un ataque cibernético es considerado como un intento no autorizado a una red programable, los ataques cibernéticos a los bancos ecuatorianos permitieron extraer información de sus clientes utilizando malware diseñado para crear amenazas en línea, dañar o explotar cualquier servicio o equipo de red. Es así como, el objetivo de este estudio se enfoca en describir e identificar las vulnerabilidades de los Bancos virtuales ecuatorianos provocadas por ciberataques entre el año 2014 y 2022, permitiéndonos realizar recomendaciones propias para mejorar la seguridad de la red. Debido a la naturaleza cualitativa del estudio, seleccionamos un estudio de caso descriptivo que analizó la escala de los ciberataques. Los ciberataques en el año 2021 ocupan el quinto lugar en términos de riesgo, convirtiéndose en un nuevo problema para los sectores tanto públicos como los privados, con la presencia de vulnerabilidades en la banca virtual de Ecuador, donde las instituciones clave reciben los fondos para fortalecer estas debilidades. Los intentos de ataque fueron en el Ministerio de Relaciones Exteriores, así como en el banco central de Ecuador, en la presidencia de la republica de Polonia, también en el Ministerio del Interior, la empresa de Telecomunicaciones de CNT y el departamento de Impuestos. La investigación de los ciberataques al sistema bancario ecuatoriano brinda un conocimiento claro de la inseguridad informática, incluyendo medidas extremas para garantizar la seguridad de la información de los clientes a través de los medios técnicos digitales para su beneficio donde también es primordial proteger los datos en sus aspectos de ciberseguridad. Los artículos que se revisaron para el análisis de los ataques cibernéticos en la banca ecuatoriana: mapeo sistemático, fueron veintiuno artículos consultados y analizados, lo cual permitió estructurar el resultado a esta investigación, donde se logró identificar que en el Banco de Guayaquil en el año 2018, tuvo un crecimiento del 57 % trayendo consigo un mayor flujo de transacciones a diferencia de los demás bancos donde para los hackers esto les llama la atención ya que hay un mayor flujo de dinero, así también se logró identificar que en el mapeo sistemático desde el año 2014 hasta el año 2022 que el rango de ataques sufrió un incremento en los años 2016, 2020 y 2022 todos estos ataques fueron por medio del malware, donde este tipo de Hackeo es un programa malicioso o código maligno que tiene como función dañar las computadoras o software, hurtar datos, sin que el usuario sepa que está sucediendo.

Palabras claves: Ciberseguridad; Ciberdefensa; phishing; malware; mapeo sistemático; ciberataques; banca ecuatoriana.

ABSTRACT

A cyber-attack is considered as an unauthorized attempt to a programmable network, cyber-attacks on Ecuadorian banks made it possible to extract information from their customers using malware designed to create online threats, damage or exploit any network service or equipment. Thus, the objective of this study focuses on describing and identifying the vulnerabilities of Ecuadorian virtual banks caused by cyber-attacks between 2014 and 2022, allowing us to make our own recommendations to improve network security. Due to the qualitative nature of the study, we selected a descriptive case study that looked at the scale of cyber-attacks. Cyber-attacks in 2021 rank fifth in terms of risk, becoming a new problem for both public and private sectors, with the presence of vulnerabilities in virtual banking in Ecuador, where key institutions receive funds to strengthen these weaknesses. The attempted attacks were on the Ministry of Foreign Affairs, as well as on the central bank of Ecuador, on the presidency of the Republic of Poland, also on the Ministry of the Interior, the CNT Telecommunications Company and the Tax department. The investigation of the cyber-attacks on the Ecuadorian banking system provides a clear understanding of computer insecurity, including extreme measures to guarantee the security of customer information through digital technical means for their benefit, where it is also essential to protect the data in their cyber security aspects. The articles that were reviewed for the analysis of cyber-attacks in Ecuadorian banking: systematic mapping, were twenty-one articles consulted and analyzed, which allowed structuring the result of this investigation, where it was possible to identify that in the Banco de Guayaquil in the year 2018, had a growth of 57% bringing with it a greater flow of transactions unlike other banks where for hackers this draws their attention since there is a greater flow of money, thus it was also possible to identify that in the systematic mapping from the year 2014 until the year 2022 that the range of attacks suffered an increase in the years 2016, 2020 and 2022 all these attacks were through malware, where this type of Hacking is a malicious program or malignant code whose function is to damage the computers or software, steal data, without the user knowing what is happening.

Keywords: Cyber security; cyber defense; phishing; malware; systematic mapping; cyber-attack; Ecuadorian bank

ÍNDICE DE LOS CONTENIDOS

1 INTRODUCIÓN 10

2 REVISIÓN DE LA LITERATURA 11

3 METODOLOGÍA 16

3.1 Métodos y técnicas empleadas en la recopilación de los datos. 16

3.2 Métodos y técnicas del análisis de los datos. 17

4 RESULTADOS 18

5 CONCLUSIÓN 25

6 REFERENCIAS 26

1 INTRODUCIÓN

Los ciberataques son considerados los problemas con más recurrencia en las redes del internet, donde por medio de las tecnologías que se ponen a disposición logran causar problemas de gran magnitud y daño a los sistemas informáticos producido por los hackers, este tipo de daño se conoce como malware el cual es utilizado con la intención de provocar un daño, o incluso explotar el dispositivo y el servicio de una red que está programada, y donde comúnmente el resultado de esta acción es la obtención de la información que se encuentra en la base de datos que esta disponible en los servidores de cada entidad bancaria, siendo así que al momento de insertar este ataques se extraen datos que son utilizados para el chantaje a sus víctimas y con esto lograr obtener grandes sumas de dinero.

Objetivo general: identificar la vulnerabilidad de la banca ecuatoriana virtual desde el año 2014 hasta el año 2022, ocasionada por los ataques cibernéticos, mediante una revisión de datos estadísticos.

Objetivos específicos:

a) Medir los ataques cibernéticos en el lapso desde el año 2014 hasta el año 2022, y el tipo de ataque que estos presentaron.
b) Comparar la ciberseguridad de la banca ecuatoriana con relación a las demás bancas de los países más cercanos.
c) Sugerir una mejora en el área de sistemas enfocada en la ciberseguridad para tener una mejor eficiencia y sostenibilidad en la Banca Ecuatoriana.

La metodología planteada fue cualitativa a través de un mapeo sistemático, que permitió la definición de las preguntas de investigación, así como la búsqueda de estudios primarios, secundarios y la selección de artículos relacionados al tema de investigación para analizar los diferentes referentes teóricos que se presentaron en el estudio, donde se propone analizar la medición de los ataques cibernéticos dentro del periodo 2014 al 2022, para posteriormente realizar una comparación, con el propósito de conocer cuáles fueron los ataques a la banca virtual ecuatoriana y el porcentaje que este reflejo, por medio de cuatro fases aplicadas en esta investigación que nos permita poder establecer un seguimiento de los datos e información recabada mediante la organización de los documentos; 1.-Delimitación de las preguntas, para poder tener claro hacia donde se encamina la investigación y que es lo que se quiere encontrar;

2.-La búsqueda bibliográfica de los diferentes autores relacionados con el tema de investigación; 3.- La selección de los documentos que proporcionen información verificable; 4.-El análisis de los documentos seleccionados.

2 REVISIÓN DE LA LITERATURA

Todo tiene un inicio en el desarrollo de la tecnología, este es un proceso que permite la actualización de nuevos medios de adaptación para el hombre, (Llamuca-Pérez, Mancheno-Saá, & Chaulisa Chaluisa, 2019) expresan que en el comienzo del siglo 20 y finales de la década de los 90, era muy frecuente ver la banca en línea, en países desarrollados" (p. 4). Dicho esto, los primeros en implementar este sistema en el año 1995, fue el banco Wells Fargo de Estados Unidos en efectuar la realización de transacciones domésticas para un mejor manejo de sus sistemas, de este modo se presentan así el significado a términos que mediante la investigación y en el ámbito de la ciberseguridad están presenten y proporcional un vistazo más claro a la investigación.

- **Ciberseguridad**

Desde la prospectiva cibernauta, se considera a la ciberseguridad como un "conjunto de variables claves, acertadamente definidas por la ITU –International Telecomunicación Unión-, en las cuales son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación" (Cano, 2008. P, 3).

- **Ciberdefensa**

"Connotación sistémica y sistemática que deben desarrollar los gobiernos, para comprender ahora sus responsabilidades de Estado, en el contexto de un ciudadano y las fronteras nacionales electrónicas o digitales" (Cano, 2008, p. 2).

- **El Phishing**

Se denomina como el "proceso por el cual una persona es contactada por email o por teléfono por alguien que simula ser una institución legítima para obtener datos privados, tales como datos bancarios, contraseñas, datos personales" (Leguizamón, 2015, p. 10).

- **Malware**

Entendemos malware como programa malicioso o código maligno que tiene como función dañar las computadoras o software, hurtar datos, sin que el usuario sepa que está sucediendo. Existen extensas diversidades de malware como: virus, troyanos, spyware, etc.

- **DDOS**

Es considerado como un ataque para privar usuarios que acceden a su red o dispositivo. La evolución de esta amenaza ataque de denegación de servicio dispensado (DDoS) es causado por generar un gran numero información de diferentes puntos voluntario para los usuarios o la organización se ve privada de sus recursos.

ATAQUES

Los ataques cibernéticos a la banca virtual al nivel mundial son algo preocupante, por tal motivo es que se debería de ejecutar protocolos de antiataques o simulaciones de ataques para evitar los fraudes, porque además de perder millones de dólares, también pueden robarles información muy confidencial a sus clientes. Es importante precisar en un marco superior que en américa latina existen varias economías fuertemente grandes, estas al tener un mayor flujo y utilización de las redes de internet son las más vulnerables a los ataques cibernéticos, tales como Brasil, Colombia y Argentina donde el porcentaje de intentos ronda en el 74%, solo en ataques de phishing, mientras que en ecuador ronda el 60 % en ataques por malware como el más alto en ataques a diferencia del Phishing.

En Ecuador, durante los últimos 5 años sufrió un incremento elevado en acceso al internet, donde mediante la búsqueda de la información se encontraron datos donde muestran que "en el año 2012 la población ecuatoriana alcanzaba el 22,5% y que en el 2015 se alcanzó el 32,8%, según estadísticas del Instituto Nacional de Estadísticas y Censo INEC 2016" (Vargas Borbúa, Reyes Chicango, & Recalde Herrera, 2017, p.36)

Estos valores son visibles cuando observamos las instituciones financieras y comerciales, tales como bancos, industrias, y turismo. Estos han aumentado sus servicios en línea teniendo un mayor flujo de información en las redes de internet que en términos simples está a merced de ciberataques, como lo es la banca electrónica, transacciones electrónicas, entre otros.

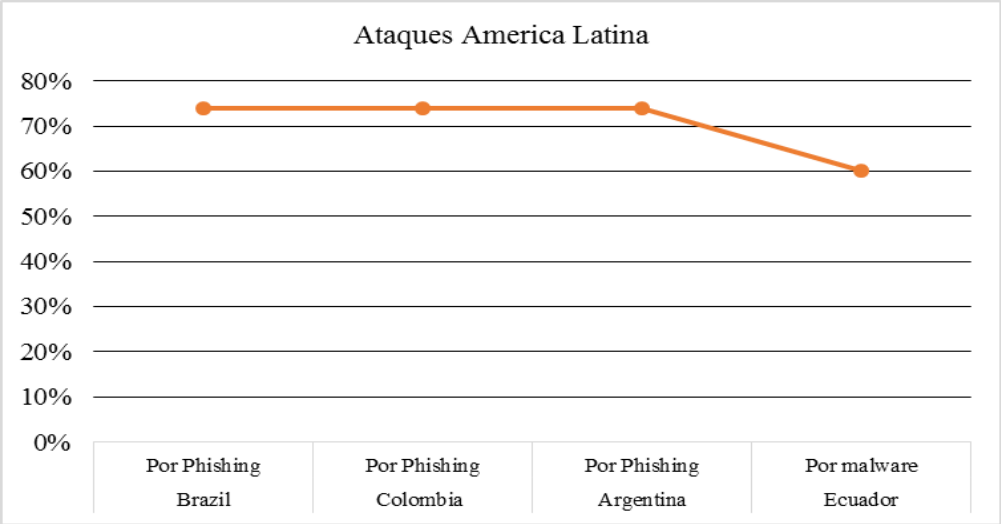


Ilustración 1Ataues Maliciosos en Países de América Latina

Fuente: Fuente: Elaboración Propia, (2023).

En este caso con el análisis de los datos presentados, se determinó que los países con mayor índice de ataques son Brasil liderando el rango, así como Colombia, Argentina y Ecuador de tal modo que estos países cuentan con un mayor flujo de dinero y una creciente expansión de los medios tecnológicos que son puestos por las entidades bancarias, como esto también se manifiestan la presencia de los ataques ya que estos países al no contar con buenos sistemas de seguridad, son más propensos a la manipulación de información de los llamados hackers.

Estos ataques cibernéticos en América Latina algunos de ellos fueron a los bancos de Ecuador como se presentaba en la ilustración anterior, así como Colombia que presentaron una perdida cuantiosa y la credibilidad de su sistema de seguridad, de manera qué “con respecto a dichos ataques a raíz de esto se tuvo que mejorar la seguridad y acceso a la información para que no se repita dicho escenario” (Góngora Jiménez & Banda Ortiz, 2021, p. 3)

Tabla 1Incremento de Internet en Redes de Servicios en Línea.

Ecuador	
Año 2012, ataques a los aspectos financieros.	22,5 %
Año 2015 ataques a los aspectos financieros.	32, 8 %

Fuente: Elaboración Propia, (2023).

La innegable introducción a la tecnología ha provocado el desarrollo y consigo la presencia de una problematización en los aspectos de la ciberseguridad. Donde en Ecuador, se puede evidenciar en sus estadísticas que las brechas de seguridad están mayoritariamente relacionadas

con el sistema financiero. Su aumento de eficiencia ha hecho que la ciberseguridad sea una preocupación, especialmente para los bancos ecuatorianos, como se mencionaba las estadísticas que pone a disposición la información de estos problemas es el Ministerio de Coordinación de Seguridad, las cuales se presentan a continuación;

Tabla 2Indice de Robo a la Banca Virtual Ecuatoriana.

Robo a la Banca Virtual Ecuatoriana	
Año 2014, con un índice del 38 % a diferencia de los años anteriores.	14 % Tarjetas de crédito. 46 % Cajeros Electrónicos.

Fuente: Elaboración Propia, (2023).

VULNERABILIDADES

Las vulnerabilidades presentes en la Banca virtual Ecuatoriana son diversas, una de ellas es la duplicación de las tarjetas emitidas por los bancos ya sean de crédito o débito, donde mediante las técnicas empleadas por los delincuentes permiten el accionar del jaqueo de cuentas, la revelación de claves personales, la utilización de páginas falsas, además de la utilización de otras técnicas como el phishing, farming, o más conocida como el fraude por correo electrónico permitiendo así el robo y uso indebido de información personal. Como lo expresan (Crespo Crespo & Ramos Chóez, Estudio del impacto financiero de las vulnerabilidades de las páginas web de los Bancos en Ecuador, 2012) “El comprador al momento de realizar el pago mediante depósito o transferencia, cree que es más seguro y eficaz porque en la actualidad no acostumbran a tener dinero en efectivo por la inseguridad por lo que utilizan este medio” (p. 12). El manejo de las herramientas tecnológicas mediante su actualización también van a permitir que los delincuentes puedan sustraer la información, de tal modo que es importante estar en constante actualización en los medios de ciberseguridad, para que los clientes tengan más segura su información y además estén conscientes de los riesgos y el accionar de sus transacciones bancarias.

Dentro de las vulnerabilidades encontradas se precisan ataques con la utilización de diversos procedimientos de phishing, donde el 31% de los casos, son por el robo de las credenciales, así también el 29% de las razones de estos ataques permiten la ex filtración de los datos en los sitios que presentan una vulnerabilidad en el sistema, por lo cual para los hackers se les facilita esto mediantes sus habilidades, observando que los usuarios utilizan por una cantidad de tiempo determinada la misma contraseña el sitio, permitiendo un ataque tanto a ese servidor como al cliente, un 30 % es para el provecho de las vulnerabilidades que los hackers encuentran en el

sistemas por supuesto encuentran las fallas técnicas en los productos de hardware y software que le facilitan el accionar, y así totalizando con un 10% otras causas que se pueden presentar mediante el ataque.

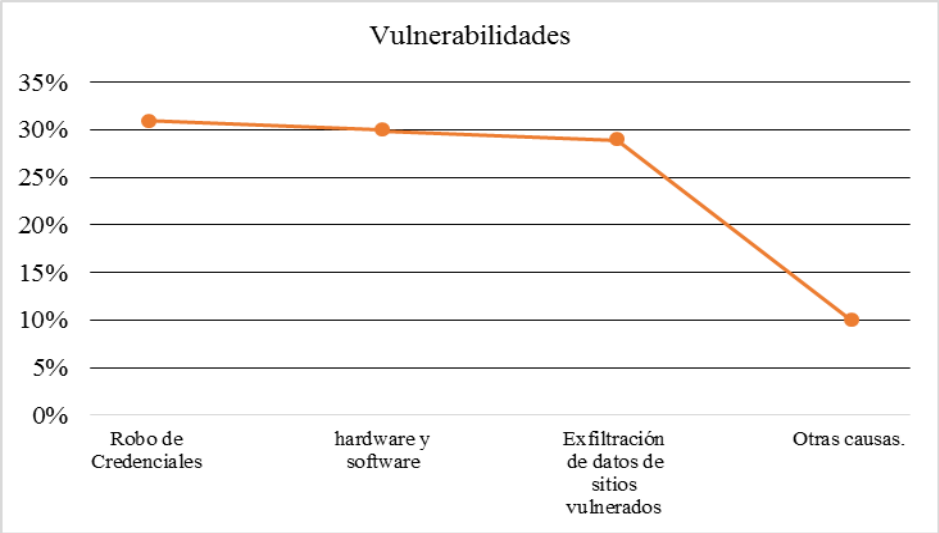


Ilustración 2Principales índices de vulnerabilidades

Fuente: Fuente: Elaboración Propia, (2023).

En este caso con la compresión y análisis de los datos presentados, se logra identificar que la mayor vulnerabilidad que presenta la Banca virtual Ecuatoriana es el robo de credenciales con un 31%, en los sistemas de hardware y software que representa a los sistemas tanto digitales como sistemas tangibles con un 29%, asociado con estos sistemas la presencia de ex filtración de datos en un 30%, y por otras causas presenten en estos medios con un 10%, por ello es preciso la constante actualización de estos medios que garanticen la seguridad de sus clientes.

SEGURIDADES

Es importante establecer seguridades dentro de todos los sistemas informáticos que tenga la presencia de datos de clientes, priorizando la información, teniendo en cuenta lo antes expresado, nuestro objetivo es poder brindar a la sociedad toda la información con respecto a la vulnerabilidad de datos que se presentan en el internet. En abrir correos electrónicos falsos con mensajes maliciosos ocasionaría perdida de su capital, información delicada, el chantaje, virus etc. Lo que se afecta por tal motivo hacemos saber a las personas que “la banca virtual es muy útil, pero también es algo peligroso por eso las personas no tienen confianza en la banca en línea” (Llamuca-Pérez, Mancheno-Saá, & Chaulisa Chaluisa, 2019, p 4).

3 METODOLOGÍA

Dada la naturaleza cualitativa de nuestra investigación, optamos por un estudio de caso descriptivo en el que se analiza inicialmente en profundidad la medición de los intentos de ataques cibernéticos desde el año 2014 al 2022, de este modo permite la obtención de información proporcionada en las diferentes fuentes digitales para poder establecer los lineamiento del trabajo que se realiza, por lo tanto se desarrollan 4 fases de investigación utilizada por, (Vargas Borbúa, Reyes Chicango, & Recalde Herrera, 2017) que permite "determinar las fases y preguntas de investigación relacionadas a los ataques cibernéticos o vulnerabilidad del sistema en cualquier plataforma financiera" (p. 39).

Fase 1: Delimitación de las preguntas de investigación, se plantean 4 preguntas.

1. ¿Cómo ha afectado los ciberataques a la banca ecuatoriana?
2. ¿Cómo saber si nuestra ciberseguridad o personal están bien capacitados para afrontar estos ataques cibernéticos?
3. ¿Cuáles fueron los más altos rangos de vulnerabilidades de la banca virtual ecuatoriana en los años del 2014 al 2022?
4. ¿Cuáles fueron las estrategias sobre la ciberseguridad y Ciberdefensa en la banca virtual ecuatoriana?

3.1 Métodos y técnicas empleadas en la recopilación de los datos.

Fase 2: Realizar la búsqueda bibliográfica.

Se plantea buscar en las bibliotecas virtuales que la Universidad Politécnica Salesiana entrega acceso a los estudiantes y docentes, Google académicos, Artículos, Revistas que son: Scielo, Fipcaec, Cienciamatria, Dialnet, entre otras. Las palabras claves de búsqueda son "Cyber Attack", "Security Banking", "Techology Banking", "types of cyber-attacks".

Fase 3: Seleccionar los documentos.

Tabla 3Criterios de Investigación

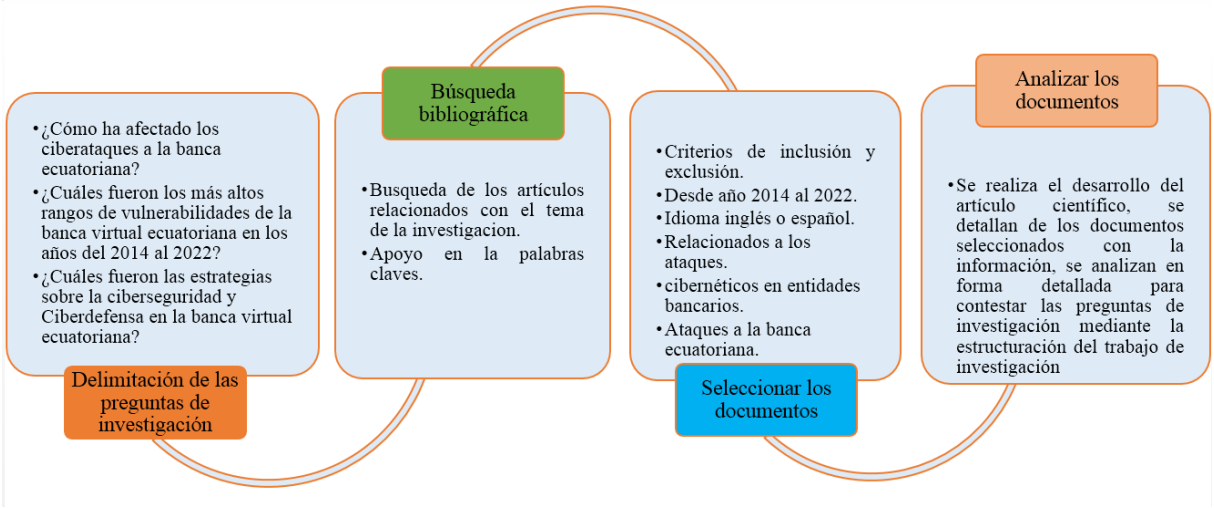
Inclusión	Exclusión
Desde año 2014 al 2022	Documentos duplicados
Idioma inglés o español	Documentos de solo resumen
Relacionados a los ataques cibernéticos en entidadesbancarios	Documentos no relacionados

Fuente: Elaboración propia, (2023).

Fase 4: Analizar los documentos.

Se realiza el desarrollo del artículo científico, se detallan de los documentos seleccionados con la información, se analizan en forma detallada para contestar las preguntas de investigación mediante la estructuración del trabajo de investigación.

Ilustración 3Metodología del proceso de investigación



Fuente: Elaboración propia, (2023).

3.2 Métodos y técnicas del análisis de los datos.

Técnica de regresión

Se empleó esta técnica de regresión para poder determinar y analizar las tendencias que se presentaron en los ataques cibernéticos en la banca virtual desde el años 2014 al 2022, lo cual permitió la búsqueda de información no solo de estos ataques a la banca virtual, sino también a redes sociales y plataformas virtuales, de este modo podemos evaluar la magnitud que posee una deficiencia en el sistema de ciberseguridad.

Por tal motivo otros países como Estados Unidos se han ofrecidos para colaborar con la ciberseguridad en nuestro y afrontar ese circunstancial dilema que afecta al país de una manera agobiante y mientras sigan ocurriendo estos ataques expuestos o no expuestos generara muchas pérdidas económicas como credibilidad a la banca ecuatoriana. Con la ayuda de otros países podemos capacitar tanto a los clientes como al personal que labora en las entidades bancarias mediante las Tecnologías de la Información, y así podemos dar un plus para que se no se genere tanta vulnerabilidad en el sistema.

4 RESULTADOS

Se puede determinar qué nuestra ciberseguridad en la banca ecuatoriana al nivel mundial deja mucho que desear. Luego de un inmensa busqueda encontramos datos y vemos que nuestro país carece de ciberseguridad, lo que incita que recibamos masivos ataques por parte de hackers, grupos informales, entre otros. Aunque sea un país que no esté muy capacitada con la ciberseguridad, no somos los únicos que países de Latinoamérica que reciben ataques a las entidades bancarias. La industria bancaria ha sido líder en la implementación del cambio tecnológico. Ha sido lento en desarrollarse en Ecuador. Sin embargo, la innovación e integración continua de las aplicaciones digitales ha llevado a mejorar los servicios financieros con los clientes en todas las aplicaciones y plataformas.

En los últimos cinco años en el Ecuador, se presentó en los medios electrónicos el aumento de su uso. Los Bancos con mayor flujo de transacciones en el año 2017 fueron, Banco Pichincha con 10.615 millones de transacciones, Banco Pacifico con 5.452 millones de transacciones, Banco Produbanco con 4.272 millones de transacciones, Banco Guayaquil con 4.024 millones de transacciones, Banco Internacional con 3.558 millones de transacciones, Banco Bolivariano con 3.115 millones de transacciones, Banco del Austro con 1.693 millones de transacciones, Banco Diners con 1.674 millones de transacciones.

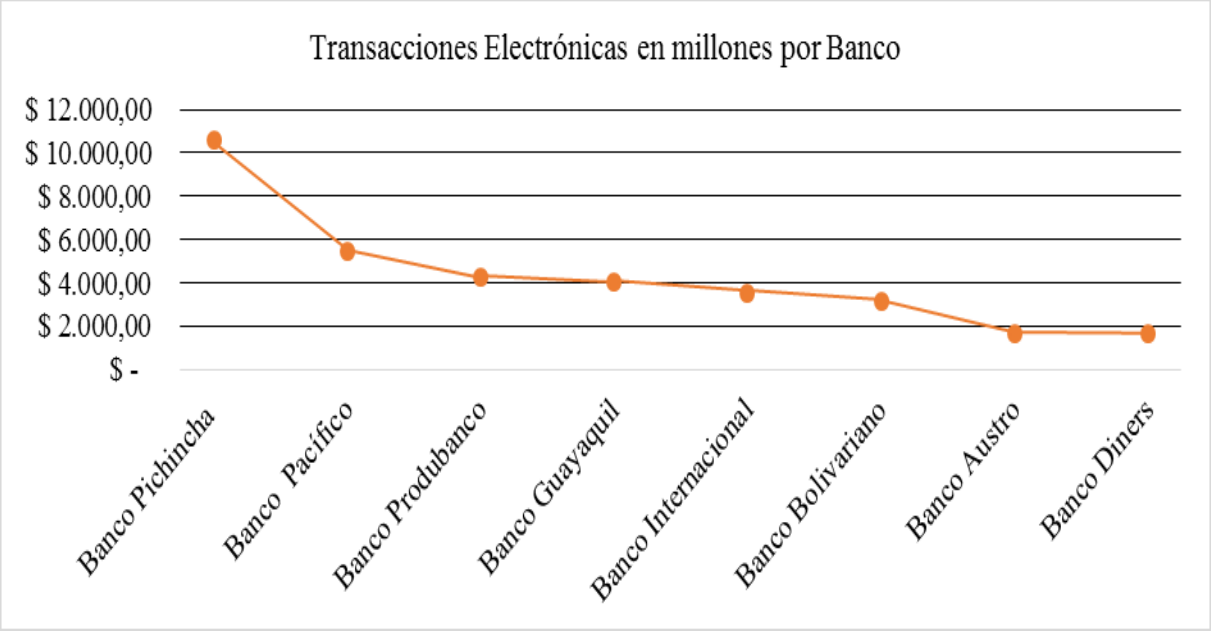


Ilustración 4Rango del Crecimiento de Transacciones Electrónicas

Fuente: Elaboración propia, (2023).

¿Cómo ha afectado los ciberataques a la banca ecuatoriana?

En este caso con la compresión y análisis de los datos, se pudo determinar que solo el 90 % de las instituciones financieras de orden público utilizan las transacciones de modo digital, pero la adopción de nuevas plataformas para llegar a más consumidores sigue siendo una tarea abierta para la industria. Las instituciones financieras actuales poseen el 90 % de los activos digitales, pero los nuevos modelos de negocios con tecnología avanzada son más riesgosos, ya que los delitos cibernéticos también aumentan y se aprovechan las defensas cibernéticas débiles. Liderando el rango de crecimiento de estos medios digitales se presenta el Banco de Guayaquil en el año 2018, trayendo consigo en este crecimiento a un mayor flujo de requerimientos bancarios en línea siendo propenso a los ataques cibernéticos que se presenten en estos sistemas, los cuales han sido más propenso en ataques de malware y phishing, ya que con un mayor flujo de información y si no se tiene la información asegurada estaría siendo observada por los hackers.

Los ataques cibernéticos se clasificaron como el quinto riesgo más alto en 2021 y se convirtieron en el nuevo estándar para los sectores público y privado, por tal motivo (Orellana Cabrera & Álvarez Galarza, 2022), expresa qué "hoy en día tener un sistema que proteja los datos de los usuarios es de suma precedencia, dado que el mínimo error facilita a los hackers tomar información de manera maliciosa e intentar venderla a terceros" (p. 12).

La mayoría de los ciberataques al país provinieron de forma externa donde el país de Brasil, Estados Unidos y el de China, estos arrojaron un promedio considerable de un máximo entre 10 a 12 ataques informáticos de hackers; siendo así que para los cyber delincuentes sus objetivos más fáciles son los sistemas que presentan varias vulnerabilidades. En este sentido, se presenta la información sobre la medición de los ataques cibernéticos dados en los últimos años.

Tabla 4 Ataques cibernéticos

Año	Suceso
2014	Se presentó un Hackeo de más de 500 millones de cuentas de Yahoo (Izaguirre Olmedo & León Gavilánez, 2018). Hackeo de cuentas de Microsoft, Facebook y Google (Izaguirre Olmedo & León Gavilánez, 2018).
2015	OEA presenta su programa de seguridad cibernética para los países del Caribe y América latina (Izaguirre Olmedo & León Gavilánez, 2018).

2016	Grupo anonymous México Hackea la página del sistema de administración tributaria de ese país (Izaguirre Olmedo & León Gavilánez, 2018). Más de un tercio de la población de Colombia reporta haber sido víctima de fraude electrónico en distintas organizaciones (Izaguirre Olmedo & León Gavilánez, 2018).
2017	Banco Central del Ecuador, se realizaron 193,3 millones de transacciones digitales (Izaguirre Olmedo & León Gavilánez, 2018).
2018	Banco Central del Ecuador, se realizaron 218,1 millones de transacciones digitales. Estafas de 16, 918 producidas por los ciber ataques en Ecuador.
2019	Apropiación fraudulenta por medios electrónicos de, 1744 Violación de la intimidad de, 2038 Acceso no concedido a sistemas informáticos de, 242 Contacto con finalidad sexual de, 165 Estafas de 18.415 producidas por los ciber ataques en Ecuador.
2020	Apropiación fraudulenta por medios electrónicos de, 2.280 en Ecuador. Violación de la intimidad de, 1.985 en Ecuador. Acceso no concedido a sistemas informáticos de, 295 en Ecuador. Contacto con finalidad sexual de, 152 en Ecuador. Estafas de 16.272 producidas por los ciber ataques en Ecuador.
2021	Apropiación fraudulenta por medios electrónicos de, 3.962 en Ecuador. Violación de la intimidad de, 1.346 en Ecuador. Acceso no concedido a sistemas informáticos de, 274 en Ecuador. Contacto con finalidad sexual de, 152 en Ecuador. Estafas de 79.784 producidas por los ciber ataques en Ecuador.
2022	Apropiación fraudulenta por medios electrónicos de, 10.393 en Ecuador. Violación de la intimidad de, 9.091 en Ecuador. Acceso no concedido a sistemas informáticos de, 1.265 en Ecuador. Contacto con finalidad sexual de, 829 en Ecuador.

Fuente: Elaboración propia, (2023).

Por los principales motivos queremos sugerir o hacerles llegar a las entidades bancarias pequeñas ideas que pueden favorecer a sus sistemas de seguridad, nuestra idea no es hacer menos al área de sistema o TI, es más una ayuda para prevenir futuros ataques. Lo que quisiéramos alcanzar es que el usuario tenga una vasta seguridad cuando ingrese a la banca digital, reciba un código en su celular o hacerle una pregunta que el solo tendrá la respuesta y así evitar que otra persona sea el que ingresa a su cuenta, también queremos que las personas o usuarios revise los correos y verificar su autenticidad de quien se lo enviar. Teniendo en cuenta los resultados anteriores también se logró identificar la vulnerabilidad de la banca virtual ecuatoriana, donde (Gobierno del Ecuador, 2019) manifestó que las principales instituciones que recibieron los intentos de intrusión fueron, “Cancillería, Banco Central, Presidencia de la República, ministerio del Interior, Servicio de Rentas Internas, CNT, varios GAD, Consejo de la Judicatura, ministerio de Telecomunicaciones y de la Sociedad de la Información, ministerio de Turismo, ministerio de Ambiente y algunas universidades” (p. 1).

¿Cuáles fueron los más altos rangos de vulnerabilidades de la banca virtual ecuatoriana en los años del 2014 al 2022?

El rango de vulnerabilidad que presentaron los intentos de ataques, fueron por malware, el cual es un tipo de software malicioso que es especialmente diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. (Olvera Morán & Campi Mayorga, 2020) expresa qué según datos de Kaspersky Lab en su informe de amenazas en tiempo real, en junio del año 2017, "Ecuador ocupó en América del Sur el primer lugar con el 2,8 % y el quinto lugar a nivel mundial en cuanto a ciberataques a sus redes" (p. 20).

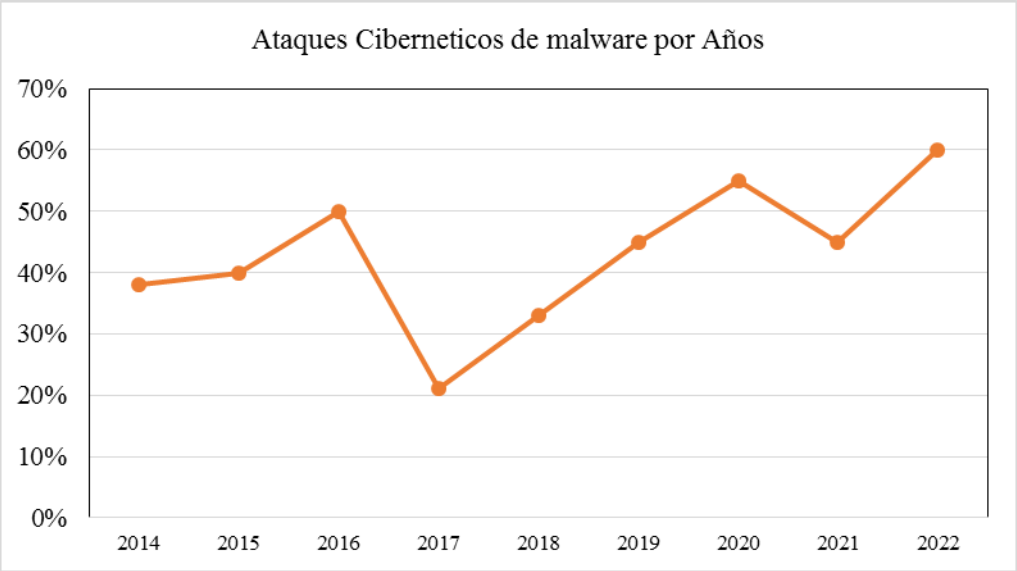


Ilustración 5Rango de Ataques Cibernéticos

Fuente: Fuente: Elaboración Propia, (2023).

En este caso con la compresión y análisis de los datos presentados, se establecen el rango de los ataques cibernéticos por años desde el 2014 hasta el 2022, donde cada uno de estos años ha presentado diferentes tipos de Hackeo ya se por tipo de hardware o malware, como estudio del caso en el año 2014 este presento el 38% de ataques de malware por sus deficientes sistemas de seguridad en la Banca virtual Ecuatoriana, en el 2015 presento un crecimiento leve del 40 % donde a pesar de los ataques presentados en el año anterior no tuvieron un índice más alto, en el año 2016 subió a un 50 % a pesar de las estrategias y ejercicios establecidos para bajar estos índices de intentos maliciosos, pero en el años 2017 estas estrategias tuvieron frutos ya que su índice de ataques bajaron al 21% siendo esta usa cifra gratificante en términos de Ciberdefensa.

Pero más tarde en el año 2018 tuvo un aumento, así como en los años 2019 con un 45%, el año 2020 con un 55 %, el año 2021 con un 45% y 2022 con un 60 % de aumento, donde estos ataques se intensificaron gracias a hackers con mayor experiencia y con los medios tecnológicos más actualizados que les permitían sustraer la información que esta sin la seguridad correspondiente.

¿Cuáles fueron las estrategias sobre la ciberseguridad y Ciberdefensa en la banca virtual ecuatoriana?

El gobierno ecuatoriano, tratando de minimizar estos problemas, tomó algunas decisiones de ciclo político, por ejemplo; formó un centro de operación estratégica de tecnología del 4 de noviembre de 2013 a las 12:00 al 5 de noviembre de 2013 a las 21:00. Donde su objetivo era controlar los ataques informáticos contra los equipos de seguridad de diversas instituciones del Estado. De modo que mediante la investigación se encontró que en Ecuador se implementó el Ecucert, que es la Agencia de Regulación y Control de las Telecomunicaciones, creador con uno de sus objetivos para el tratamiento de los incidentes Informáticos, el cual inicio a comienzos del año 2012.

Así también implemento una seria de Políticas sustentables, una de ellas fue el Acuerdo Ministerial No. 166, que se emitió desde la secretaria nacional de la administración pública, donde se les obligaba a las instituciones de orden público que implementen el esquema gubernamental presentado anteriormente.

Tabla 5Estrategia propia de ciberseguridad y Ciberdefensa

ECURET Agencia de Regulación y Control de las Telecomunicaciones	Acuerdo Ministerial No. 166.
Centro de Prevención de Accidentes Informáticos de la Autoridad de Regulación y Control de las Telecomunicaciones del Ecuador.	Esquema Gubernamental de Seguridad de la Información EGSI. De 19 de septiembre de 2013.

Tratamiento de los incidentes Informáticos ✓ Alerta de seguridades. ✓ Control de seguridades. ✓ Coordinación y respuesta.	Mediante acuerdos ministeriales N° 804 y 837 del Ministerio de 29 de julio y 19 de agosto de 2011, la Secretaría de Administración del Estado conformó la Comisión de Seguridad de la Información y Tecnologías de la Información y las Comunicaciones, que integra representantes del Ministerio de Telecomunicaciones y del Ministerio. De información. Sociedad, la Secretaría de Inteligencia y la Secretaría de la Función Pública, debiendo definir dentro de sus lineamientos para la seguridad de la información y protección de la infraestructura informática. (Archivos de la etiqueta: Derecho Informático Ecuador, 2021)

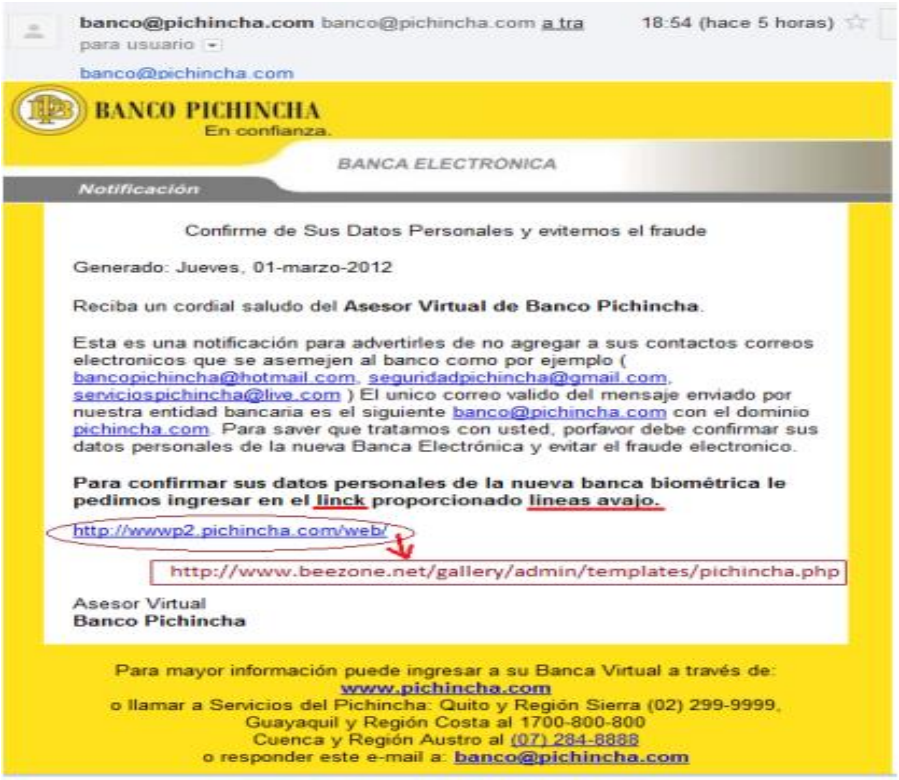
Fuente: Elaboración Propia, (2023).

¿Cómo saber si nuestra ciberseguridad o personal están bien capacitados para afrontar estos ataques cibernéticos?

El personal o ciberseguridad debe de estar muy atento a cualquier anomalía que se presente el sistema bancario, para que esto suceda se debe de realizar constantes capacitaciones e informar sobre la actualización solo al personal autorizado y encargado del banco.

Robos por correo electrónico

Los correos que les llegan a los usuarios son similares a los del asesor virtual del banco pichincha, en donde se advierte de no agregar a sus contactos direcciones de correo que se asemejen a las siguientes cuentas con dominios de bancopichincha@hotmail.com, seguridadpichincha@gmail.com, serviciospichincha@live.com, si seguimos leyendo el correo nos encontramos al final del mensaje con un pequeño párrafo, que si nos fijamos bien vamos a toparnos con faltas ortográficas (linck y no link, avajo en lugar de abajo, saver en lugar de saber (Crespo Crespo & Ramos Chóez, 2012, pag. 133).



Fuente: Toma de (Crespo Crespo & Ramos Chóez, 2012)

¿Cúal sería una mejora para que los sistemas enfocados en la ciberseguridad tengan una mejor eficiencia y sostenibilidad en la Banca Ecuatoriana?

Desde un punto de vista al problema que se presenta en la banca virtual ecuatoriana, una mejora sería que las entidades bancarias con mayor flujo y utilización de sus portales virtuales, automáticos se asocien con empresas extranjeras que ofrecen un servicio de ciberseguridad más actualizado y con mejores accesos, para que así también se pueda garantizar el resguardo de la información de los clientes y una mejor facilidad de uso, para que así se logre prevenir futuros ataques. Lo que quisiéramos alcanzar y proponer de manera hipotética es que el usuario tenga una vasta seguridad cuando ingrese a la banca digital, reciba una llamaba personalizada y autorizada por el banco además del código en su celular, también hacerle una pregunta de verificación donde solo el dueño tendrá la respuesta y así evitar que otra persona sea el que ingresa a su cuenta, también queremos que las personas o usuarios revisen los correos electrónicos y verifiquen su autenticidad de quien se lo envían ya que también por este medio se sustrae información, de igual forma se sugiere en este punto que las entidades bancarias

informen a sus clientes sobre estos intentos y como se efectúan para que así tengan un mayor conocimiento y estén más prevenidos.

5 CONCLUSIÓN

La investigación sobre los ataques cibernéticos en la Banca Ecuatoriana, permite una visión clara en el sentido de seguridad informática a la incorporación de medidas extremas que garanticen el resguardo de la confidencialidad de sus clientes que utilizan los medio digitales para su beneficio y resguardo de datos, como bien sabemos los ataques cibernéticos se incrementaron a medidas por la enfermedad de COVID-19 como se presentaron en los datos de los ataques por año, dado que se utilizaba la internet con más frecuencia, se hacía todo tipo de trámites bancarios sin la seguridad necesaria y eso facilitaba a los atacantes sustraer los datos para cometer sus crímenes sin que el usuario supiera que conocían su información.

También podemos concluir que se logró identificar que la mayor vulnerabilidad que presenta la Banca virtual Ecuatoriana es el robo de credenciales, con un 31% de índice en los sistemas de hardware y software por ello es primordial establecer planes de mejoras en conjuntos con gobiernos para la implementación de nuevas tecnologías para ayuden el aseguramiento de la información de los clientes, con respecto a la banca ecuatoriana se presentó un rango de los ataques cibernéticos por años desde el 2014 hasta el 2022, donde cada uno de estos años se suscitaron diferentes tipos de Hackeo ya sea por tipo de hardware o malware, y que dio como respuesta al estudio establecido que en el año 2014 el 38% de ataques fueron de malware por sus deficientes sistemas de seguridad en la Banca virtual Ecuatoriana, en el 2015 presento un crecimiento leve del 40 % donde a pesar de los ataques presentados en el año anterior no tuvieron un índice más alto, en el año 2016 subió a un 50 % a pesar de las estrategias y ejercicios establecidos para bajar estos índices de intentos maliciosos, pero en el años 2017 estas estrategias tuvieron frutos ya que su índice de ataques bajaron al 21% siendo esta usa cifra gratificante en términos de Ciberdefensa.

También se señaló que el Gobierno de Ecuador implementó el Centro de Respuesta a Incidentes Informáticos de la Autoridad de Regulación y Control de Telecomunicaciones de Ecuador, Ecucert, cuya misión principal es apoyar la prevención y resolución de accidentes y seguridad de información, a través de la coordinación, sensibilización y soporte técnico, para el tratamiento de los incidentes Informáticos, iniciado a partir del año 2012. Así también implemento una seria de Políticas sustentables, una de ellas fue el Acuerdo Ministerial No. 166,

que se emitió desde la secretaria nacional de la administración pública, donde se les obligaba a las instituciones de orden público que implementen el esquema gubernamental presentado anteriormente.

6 REFERENCIAS

Echeverría Joniaux, M. V., Garaycoa Walker, M. A., & Tusev, A. (2020). ¿Estan Preparados los Millennials Ecuatorianos contra un ataque Informático? *Revista de Ciencias Sociales y Humanidades chakiñan*. Obtenido de https://chakinan.unach.edu.ec/index.php/chakinan/article/view/366

Ghelani, D., Kian Hua, T., & Reddy Koduru, S. K. (2022). *Posted on Authorea 22 Sep 2022 — CC-BY 4.0 — https://doi.org/10.22541/au.166385206.63311335/v1 — This a preprint and has not been peer reviewed. Data may be preliminary.Cyber Security Threats, Vulnerabilities, and Security SolutionsModels in Banking.* Institute of Computer Science, Gujrat Technological University. Obtenido de https://www.researchgate.net/publication/363786499_Cyber_Security_Threats_Vulnerabilities_and_Security_Solutions_Models_in_Banking

Gobierno del Ecuador. (2019). *Mas de 40 millones de de ataques al Ecuador neutralizados desde el retiro del asilo de Julian Assange.* Quito: Gobierno Electrónico. Obtenido de https://www.gobiernoelectronico.gob.ec/mas-de-40-millones-de-ataques-al-ecuador-neutralizados-desde-el-retiro-del-asilo-a-julian-assange/

Leyva Méndez, A. E. (2021). *Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano.* Obtenido de file:///C:/Users/Billy%20Avila/Downloads/Dialnet-AnalisisDePoliticasPublicasDeSeguridadCiberneticaE-7926828.pdf

Ojeda Contreras, F. I., Moreno-Narváez, V. P., & Torres Palacios, M. M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*. Obtenido de https://cienciamatriarevista.org.ve/index.php/cm/article/view/366

Olvera Morán, M. Y., & Campi Mayorga, I. I. (2020). Análisis de Ataques Cibernéticos hacia el Ecuador. *Coordinación de Investigación Desarrollo Tecnológico e Innovación*, 75. Obtenido de https://revistacientificaistjba.edu.ec/images/joomgallery/details/gallery_2/gallery_1_9/Edicion_Mayo_2020_COMPLETO-c.pdf#page=19

Vargas Borbúa, R., Reyes Chicango, R., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO. Revista LAtinoamericana de Estudios de Seguridad*. Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/view/2571

Aguilar Antonio, J. M. (2019). *Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad.* URVIO Revista Latinoamerica de Estudios de Seguridad. Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/view/4007

Airehrour, D., Vasudevan Nair, N., & Madanian, S. (2018). *Ataques de ingeniería social y contramedidas en el sistema bancario de Nueva Zelanda: avance de un modelo de mitigación que refleja al usuario.* Instituto de Tecnología Nelson Marlborough, Nueva Zelanda. Obtenido de https://www.mdpi.com/2078-2489/9/5/110

Archivos de la etiqueta: Derecho Informático Ecuador. (2021). *Etiqueta: Derecho Informático Ecuador*. Obtenido de https://www.informatica-juridica.com/etiqueta/derecho-informatico-ecuador/

Cano, J. (2008). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas*, 4. Obtenido de https://acis.org.co/archivos/Revista/119/Editorial.pdf

Crespo Crespo, M. A., & Ramos Chóez, R. E. (2012). *Estudio del Impacto Financiero de las Vulnerabilidades de las Páginas Web de los Bancos en Ecuador.* Universidad Politénica Salesiana Sede Guayaquil. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/3223/1/UPS-GT000334.pdf

Crespo Crespo, M. A., & Ramos Chóez, R. E. (2012). *Estudio del impacto financiero de las vulnerabilidades de las páginas web de los Bancos en Ecuador.* Repositorio Institucional de la Universidad Politécnica Salesiana, Guayaquil. Obtenido de https://dspace.ups.edu.ec/handle/123456789/3223

E catota, f., Morgan, G., & C enfermo, d. (2018). Capacidades de respuesta a incidentes de ciberseguridad en el sector financiero ecuatoriano. *Revista de Ciberseguridad*. Obtenido de https://academic.oup.com/cybersecurity/article/4/1/tyy002/4990518

Gilces Zambrano , A. F., Demera Centeno, V., & Vaca Cárdenas, L. (2021). Mecanismos de ciberseguridad basados en honeypots. *Revista de Tecnologías de la Informática y las Telecomunicaciones*. Obtenido de https://webcache.googleusercontent.com/search?q=cache:mphhLw5qrVIJ:https://revistas.utm.edu.ec/index.php/Informaticaysistemas/article/download/3708/3958/&cd=1&hl=es&ct=clnk&gl=ec

Góngora Jiménez, S. R., & Banda Ortiz, H. (2021). Impacto en el precio de las acciones de los bancos debido al ataque cibernético al SPEI. *Panorama Económico*. Obtenido de https://panoramaeconomico.mx/ojs/index.php/PE/article/view/66

Izaguirre Olmedo, J., & León Gavilánez, F. (2018). Análisis de los ciberataques realizados en América Latina. *Universidad Internacional del Ecuador*. Obtenido de https://revistas.uide.edu.ec/index.php/innova/article/view/837

Leguizamón, M. M. (2015). *El phishing.* Universitat Jaume I. Departament de Llenguatges i Sistemes Informàtics. Obtenido de http://hdl.handle.net/10234/127507

Llamuca-Pérez, S. L., Mancheno-Saá, M. J., & Chaulisa Chaluisa, S. (2019). E-banking, una necesidad de virtualización en el sector financiero ecuatoriano. *Revista Científica FIPCAEC*. Obtenido de https://fipcaec.com/index.php/fipcaec/article/view/155

Orellana Cabrera, X. E., & Álvarez Galarza, M. D. (2022). *Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019.* Universidad Católica de Cuenca. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8399852

Perdigón Llanes, R., & Pérez Pino, M. T. (2022). Análisis holístico del impacto social de los negocios electrónicos en América Latina, de 2014 a 2019. *PAAKAT: Revista de Tecnología y Sociedad*. Obtenido de http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/459

Souza Barbosa, J., Borges y Silva, D., Cabral de Oliveira, D., Cabral de Jesús, D., & Flavio de Miranda, W. (2021). Protección de datos y seguridad de la información en la pandemia COVID-19: contexto nacional. *Investigación. Sociedad y Desarrollo*. Obtenido de https://rsdjournal.org/index.php/rsd/article/view/12557