UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

EL PHISHING COMO RIESGO INFORMÁTICO, TÉCNICAS Y PREVENCIÓN EN LOS CANALES ELECTRÓNICOS: UN MAPEO SISTEMÁTICO

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

AUTOR: LUIS FERNANDO ROSERO TEJADA

TUTOR: JOE FRAND LLERENA IZQUIERDO

Guayaquil – Ecuador

2021

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Luis Fernando Rosero Tejada con documento de identificación N° 0921686861 manifiesto que:

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

Guayaquil, 15 de septiembre del año 2021

Atentamente,

Luis Fernando Rosero Tejada
C.I. 0921686861

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

Luis Fernando Rosero Tejada con documento de identificación No. 0921686861, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo académico: El phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático, el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

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

Guayaquil, 15 de septiembre del año 2021

Atentamente,

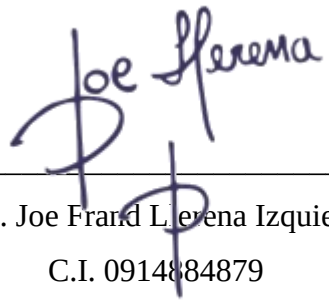
Luis Fernando Rosero Tejada
C.I. 0921686861

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: El phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático, realizado por Luis Fernando Rosero Tejada con documento de identificación N° 0921686861, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 15 de septiembre del año 2021

Atentamente,



Ing. Joe Frand Llerena Izquierdo, MSig.
C.I. 0914884879

El phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático

Luis Rosero-Tejada[1][0000-0002-0290-7517] and Joe Llerena-Izquierdo[2][0000-0001-9907-7048]

[1]Universidad Politécnica Salesiana Guayaquil, Ecuador
lroserot@est.ups.edu.ec, jllerena@ups.edu.ec

Abstract. In electronic channels, the flow of information is permanent, as most transactions and information inquiries are carried out digitally, the threats of computer risks grow. The problem with these is that they are serious because they become computer crimes, they threaten all users who use the internet for their daily activities, they affect business and economic-financial activities. The objective is to give the necessary importance to phishing, to create familiarity with its meaning and what must be done for its correct prevention. A quantitative descriptive analytical methodology and the systematic mapping technique are used to review academic content web portals and phishing-related material with their characteristics. The results allow viewing the statistical information and the growth of phishing in the last six years and the provinces with the highest number of cases; An impact matrix is generated according to the highest percentages in relation to complaints and prevention strategies are indicated. It is concluded that phishing is a growing computer risk therefore it is necessary to prevent educate and train to be able to mitigate it.

Keywords: Phishing, cybercrime, cybersecurity.

Resumen. En los canales electrónicos el flujo de información es permanente, a medida que la mayoría de las transacciones y consultas de información se realizan de manera digital, crecen las amenazas de riesgos informáticos. El problema de estos es que son graves porque se convierten en delitos informáticos, amenazan a todos los usuarios que utilizan el internet para sus actividades diarias, afectan a los negocios y actividades económicas-financieras. El objetivo es darle la importancia necesaria al phishing, crear familiaridad con su significado y que es lo que se debe de realizar para su correcta prevención. Se utiliza la metodología analítica descriptiva de corte cuantitativo, y la técnica del mapeo sistemático para una revisión de los portales web de contenido académico y el material relacionado al phishing con sus características. Los resultados permiten visualizar la información estadística y el crecimiento del phishing en los últimos seis años y las provincias con un mayor número de casos; se genera una matriz de impacto según los porcentajes más altos con relación a las denuncias y se señalan las estrategias para la prevención. Se concluye que el phishing es un riesgo informático creciente por ende es necesario prevenir: educar y capacitar para poder mitigarlo.

Palabras clave: Phishing, delitos informáticos, ciberseguridad.

1 Introducción

A nivel mundial, con el comienzo de la pandemia de COVID-19, los criminales han aprovechado el cambio del modelo laboral, el teletrabajo, que permite a los empleados conectarse remotamente a los sistemas de sus organizaciones. Así instituciones de salud han sido atacadas y sitios web que tienen contenido relacionado al COVID-19 fueron creados para efectuar actividades de phishing [1–4]. Las empresas con más altos niveles organizacionales, proporcionaron mejores normas de seguridad electrónica, las cuales fueron orientadas principalmente al uso de VPN (Red Privada Virtual), a evitar conexiones inalámbricas inseguras; las normas que tuvieron menor atención fueron: el bloqueo del equipo, los correos de phishing y actualizaciones de software [5–7].

Dado el incremento de los negocios en línea, en las transacciones de grandes corporaciones y los gobiernos, el cibercrimen los puso en la mira. Los departamentos de TI (Tecnología de la información) han incrementado sus esfuerzos para evitar ataques a sus instituciones [8][9]. La interpol predice un incremento del 59% de los ataques de phishing con una tendencia al alza en los meses siguientes desde que comenzó la pandemia en el año 2020 [10–12].

El problema es que este tipo de riesgos son graves porque se convierten en delitos informáticos, amenazan a todos los usuarios que utilizan el internet para sus actividades diarias, por el desconocimiento general sobre los mismos [13][14]. Según la constitución del Ecuador en el Código Orgánico Integral Penal (COIP), reformado en el 2014, en los artículos referentes, mejora la legislación con respecto a los delitos informáticos, en los que se incluye el phishing. Esta modificación ayuda a la disuasión de las personas que quieran cometer actos ilícitos ya que está sancionado con una pena privativa de libertad de 1-3 años [15][16][17].

Se plantea la siguiente pregunta de investigación: ¿Por qué es necesaria la prevención del phishing en los canales electrónicos?

Para detectar y evitar a tiempo que los riesgos informáticos se conviertan en delitos informáticos, a su vez conocer su alcance y como las estadísticas permiten cuantificar la situación real y establecer las soluciones correctas.

El objetivo de este trabajo es evidenciar la importancia de la prevención necesaria al phishing, crear familiaridad con su significado y que es lo que se debe de realizar para su correcta mitigación.

2 Materiales y Métodos

Se utiliza la metodología analítica descriptiva de corte cuantitativo, y la técnica del mapeo sistemático para una revisión rigurosa de los portales web, bases de datos indexadas y sitios de organismos gubernamentales de contenido público y académico,

así como el material relacionado al phishing con sus características de alta relevancia en la actualidad. Se utiliza la técnica del mapeo sistemático con la revisión de bibliografía entre los años 2016 al 2021 con énfasis en el tiempo de la pandemia del COVID-19.

2.1 Materiales

El phishing es una variación de ataque de ingeniería social, en el cual su objetivo es aprovechar debilidades que se encuentran en procesos de sistema y que son motivados por los usuarios del Sistema. El término phishing hace referencia a la palabra fishing; el comienzo del cambio de las letras "ph" por la "f" se debe a que uno de los primeros tipos de hacking estaba enfocado en las redes de telefonía, esto se lo conoce como "phone phreaking" por lo tanto "ph" terminó reemplazando a la letra "f" [18][19][20].

Los tipos de phishing que existen actualmente son:

- Phishing regular o tradicional, este tipo de phishing es el más común, el usuario recibe un correo donde le indican acceder a un enlace que es un sitio web falso o también solicita en el mismo correo enviar información confidencial con motivo de actualización de datos [21].
- Phishing basado en malware, cuando se recibe el correo, este tiene archivos adjuntos que tiene el software malicioso o indica un link que hace referencia a descargar un archivo infectado [22].
- Spear phishing está direccionado a un negocio o a una persona en específico en la empresa, el atacante tiene información acerca de la víctima, el cual utiliza para engañar y solicitar información sensible [23].
- Vishing se realiza mediante llamadas telefónicas, VoIP (llamadas voz sobre ip), indicando a la víctima que llame a un número específico que pretende ser una empresa, para proceder a dar su información [24].
- Smishing se envía a los teléfonos celulares un SMS ofreciendo algún tipo de beneficio, premio u oportunidad laboral, esto es aplicado actualmente a programas de mensajería como Facebook Messenger, Instagram, WhatsApp, Telegram [25].
- Pharming se cambia el acceso al sitio web a uno falso por medio de cambios en los dns del servidor o se dirige el tráfico a una dirección ip falsa, en este el usuario ingresa sus credenciales [26].
- Ceo suplantador consiste en que la dirección de correo electrónico es suplantada con el fin de transferencias de dineros, solicitándolas a trabajadores específicos en la empresa [27].

La creciente conectividad de los dispositivos electrónicos que se utilizan para distintos propósitos como el trabajo, salud y ocio permite una posible brecha de seguridad. A medida que la internet de las cosas (IOT) se hace más común y los dispositivos permiten estar conectados permanentemente, una de las desventajas es que, si estos dispositivos no tienen la seguridad correspondiente, los ataques de phishing se realizan a uno de estos dispositivos, el cual queda comprometido y guarda la información sensible del usuario como las claves de acceso y credenciales [28].

Los hackers aprovechan las vulnerabilidades de los dispositivos IOT, esto podría ocurrir con el envío de una señal a un dispositivo conectado dentro la red como por ejemplo impresoras, asistentes virtuales de voz, sistemas inalámbricos de sonido, etc. El problema es que esto no es prevenido a tiempo y la mayor parte de las organizaciones no capacitan a sus trabajadores en los ataques actuales de phishing y cómo proceder ante las variaciones de este. También es muy importante que las computadoras, celulares y todo tipo de dispositivo IOT tenga las actualizaciones de seguridad correspondientes, esta es una de las formas de reforzar la seguridad, en algunas compañías se les dificulta suministrar las actualizaciones a los dispositivos mencionados y algunos no tienen esta característica disponible [29].

Por otra parte, las redes sociales están más propensas a sufrir contenido malicioso, el phishing es uno de los problemas que afectan a las cuentas de los usuarios, cuando el usuario accede a este tipo de contenido malicioso, se compromete la información y es más probable que los contactos accedan a enlaces de alguien conocido dentro de la red social, lo cual los vuelve vulnerables al phishing [30].

2.2 Métodos

En el presente artículo académico se emplea la metodología de mapeo sistemático [31] el cual permite obtener de una forma más específica la información necesaria sobre el phishing, su concepto y clasificación, de esta manera se puede obtener un conocimiento más amplio del tema.

Etapa 1: Definir pregunta de investigación.
Se formula la pregunta para guiar el resto de las etapas, como se detalla a continuación en la Tabla 1.

Table 1. Pregunta y motivo de investigación

Pregunta	**Motivo**
¿Cómo se utiliza la bibliografía científica sobre el phishing desde el año 2016 al año 2021?	Precisar la información necesaria para el desarrollo del trabajo académico.

Para los criterios de inclusión y exclusión se utilizaron los siguientes enunciados, como se detalla a continuación en la Tabla 2.

Table 2. Criterios de inclusión y exclusión

Criterios de Inclusión	**Criterios de Exclusión**
Toda publicación científica tiene que ser admisible para su inclusión en el presente trabajo si tiene referencia a conceptos, clasificaciones, herramientas y metodologías	Se excluyeron trabajos de investigación que no cumplían con los requisitos mínimos
Se incluyen trabajos cuantitativos y cualitativos	Se excluyeron trabajos donde el objetivo no estuviera alineado al tema principal.
Se incluyen trabajos en inglés y español	Se excluyeron trabajos en otros idiomas

Etapa 2: Realizar la búsqueda bibliográfica.
La investigación bibliográfica se realizó en las plataformas SCIENCE DIRECT, SCOPUS y IEEE XPLORE; fueron utilizados los términos: phishing AND phishing attacks AND phishing detection; fueron tomados en cuenta trabajos científicos a partir del año 2016 que hagan referencia a los términos mencionados.

3 Resultados

3.1 Reconocimiento de los trabajos científicos en las plataformas web sobre el phishing

Etapa 3: Elegir las referencias.
Hasta el sábado 15 de mayo del 2021, fecha de aplicación de los filtros, los resultados están sujetos a cambios por los nuevos artículos que se añaden a la plataforma.

Se realiza la búsqueda de los términos en las plataformas de SCOPUS, IEEE EXPLORE y SCIENCE DIRECT. En la plataforma SCOPUS el resultado son 631 documentos, en los cuales se utilizó los filtros correspondientes el resultado de este son 74 documentos. Por otro lado, en la plataforma IEEE EXPLORE el resultado son 257 documentos, empleando los filtros correspondientes el resultado son 20 documentos. Para finalizar, en la plataforma SCIENCE DIRECT el resultado son 198 documentos, como complemento de los filtros correspondientes el resultado son 68 documentos, como se detalla a continuación en las tablas 3, 4 y 5.

Table 3. Términos de búsqueda en SCOPUS

Fases de búsqueda	Proceso de búsqueda
Fase 1	(TITLE-ABS-KEY (phishing) AND TITLE-ABS-KEY (phishing AND attacks) AND TITLE-ABS-KEY (phishing AND detection)); Resultado: 631 documentos
Fase 2	AND (LIMIT-TO (DOCTYPE , "ar")); Resultado: 278 documentos
Fase 3	AND (LIMIT-TO (SUBJAREA , "COMP")); Resultado: 207 documentos
Fase 4	AND (LIMIT-TO (OA , "all")) ; Resultado: 74 documentos

Table 4. Términos de búsqueda en IEEE EXPLORE

Fases de búsqueda	Proceso de búsqueda
Fase 1	((("All Metadata":phishing) AND "All Metadata":attacks) AND "All Metadata":detection); Resultado: 257 documentos
Fase 2	((("Index Terms":phishing) OR "Index Terms":attacks) OR "Index Terms":detection); Re-sultado: 162 documentos
Fase 3	((("Document Title":phishing) OR "Document Title":attacks) OR "Document Ti-tle":detection); Resultado: 20 documentos

Table 5. Términos de búsqueda en SCIENCE DIRECT

Fases de búsqueda	Proceso de búsqueda
Fase 1	Title: phishing: 198 documentos
Fase 2	Title: phishing attacks: 124 documentos
Fase 3	Title: phishing detection: 68 documentos

3.2 Categorización de los contenidos científicos sobre phishing por medio del mapeo sistemático

Etapa 4: Ordenar las referencias.
La categorización usó filtros generales y específicos, se detalló los términos para las búsquedas en los portales web de SCOPUS, IEEE XPLORE y SCIENCE DIRECT, esto se visualiza en la figura 1.

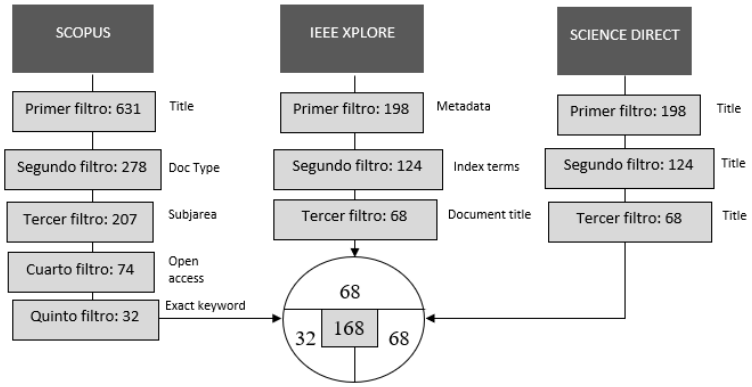


Fig. 1. Búsqueda de contenido científico

3.3 Análisis de los resultados sobre la revisión sistemática

Pregunta de investigación: ¿Cómo se utiliza la bibliografía científica sobre el phishing desde el año 2016 al año 2021? Los resultados especifican que la bibliografía científica acerca del phishing es mayor en la plataforma de SCOPUS, el período abarca desde el año 2016 hasta el año 2021, se nota un incremento en el 2020 por motivo de la pandemia del COVID-19. De acuerdo con la tabla 6 se mencionan los resultados.

Table 6. Bibliografía científica de las plataformas

AÑO	SCOPUS	IEEE	SCIENCE DIRECT
2016	70	34	36
2017	84	37	28
2018	99	38	27
2019	154	55	37
2020	179	78	49
2021	45	15	21

3.4 Analizar la evolución del phishing y sus modalidades para la generación estadística histórica utilizando una revisión de trabajos científicos previos

La información estadística proporcionada por la Fiscalía General del Estado permite conocer los datos sobre los delitos informáticos actuales que están enmarcados en el COIP (Código Orgánico Integral Penal) existen nueve de ellos. A continuación, la tabla 7 menciona lo antes indicado.

Table 7. Tipos de delitos informáticos en Ecuador

Referencia COIP	**Tipo Delito**
Artículo 212	Suplantación de identidad
Artículo 328	Falsificación y uso de documento falso
Artículo 190	Apropiación fraudulenta por medios electrónicos
Artículo 234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones
Artículo 173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos
Artículo 232	Ataque a la integridad de sistemas informáticos
Artículo 230	Interceptación ilegal de datos
Artículo 231	Transferencia electrónica de activo patrimonial
Artículo 229	Revelación ilegal de base de datos

Fuente: http://biblioteca.defensoria.gob.ec/handle/37000/2722

La información se ha clasificado por el número de denuncias a nivel nacional, a nivel geográfico en las veinticuatro provincias del Ecuador, detallado en la tabla 8.

Table 8. Phishing según provincias año 2020

Provincia	**Año 2020**
Azuay	155
Bolívar	25
Cañar	15
Carchi	26
Chimborazo	49
Cotopaxi	48
El Oro	165
Esmeraldas	44
Galápagos	7
Guayas	1473
Imbabura	82
Loja	82
Los Ríos	56
Manabí	171
Morona Santiago	11

Napo	7
Orellana	23
Pastaza	8
Pichincha	1236
Santa Elena	36
Santo Domingo De Los Tsáchilas	56
Sucumbíos	27
Tungurahua	121
Zamora Chinchipe	15
Total	3938

Fuente: Fiscalía General del Estado

Por otro lado, la figura 2 muestra un resultado por provincias, en el cual se puede observar que entre las provincias de Guayas y Pichincha suman el 68.79% de los casos a nivel nacional del Ecuador en el año 2020.

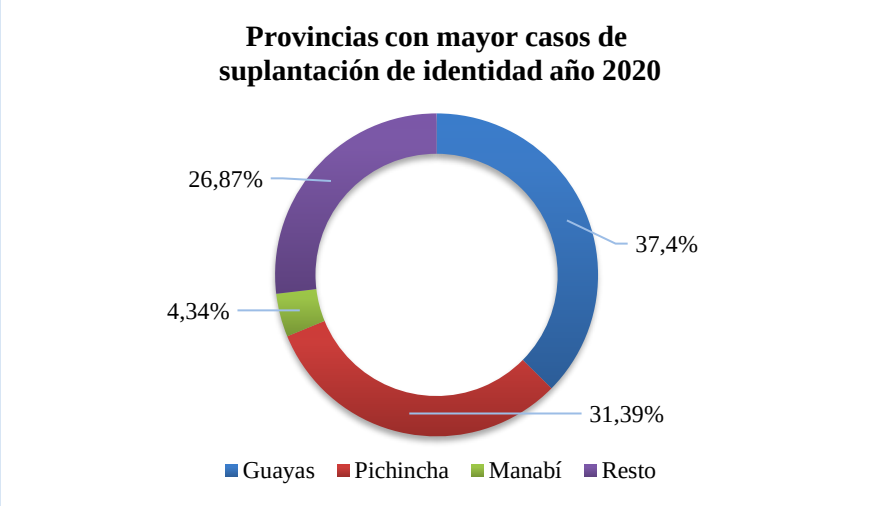


Fig. 2. Provincias con mayor casos phishing en el 2020

Por consiguiente, la figura 3 muestra la evolución del delito de suplantación de identidad en el período 2014-2020. Así, la tasa de crecimiento promedio anual fue de 13.2% en dicho período, pero con tendencias diferenciadas. En efecto, entre 2014-2015, hay un aumento significativo de 189%, mientras que en 2017 disminuye levemente en 11.6% para volver a crecer de manera importante en un 38.7% en 2018 y 10.1% en 2019 y reducirse en 14.4% en 2020, por ser el primer año de la pandemia y menor número de transacciones económicas y financieras.

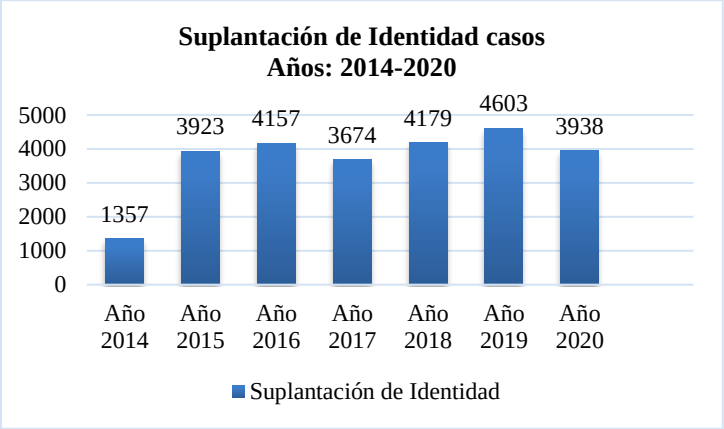


Fig. 3. Phishing en el período 2014-2020

Para finalizar, la figura 4 muestra la clasificación de delitos informáticos con mayor número de denuncias en el período 2018-2020, mostrando la evidencia que el phishing (suplantación de identidad) es el principal (número uno) en los delitos informáticos en el Ecuador. Siendo, en promedio anual en dicho periodo, el 43,2% visto de esta forma de 10 delitos informáticos 4 corresponden al phishing.

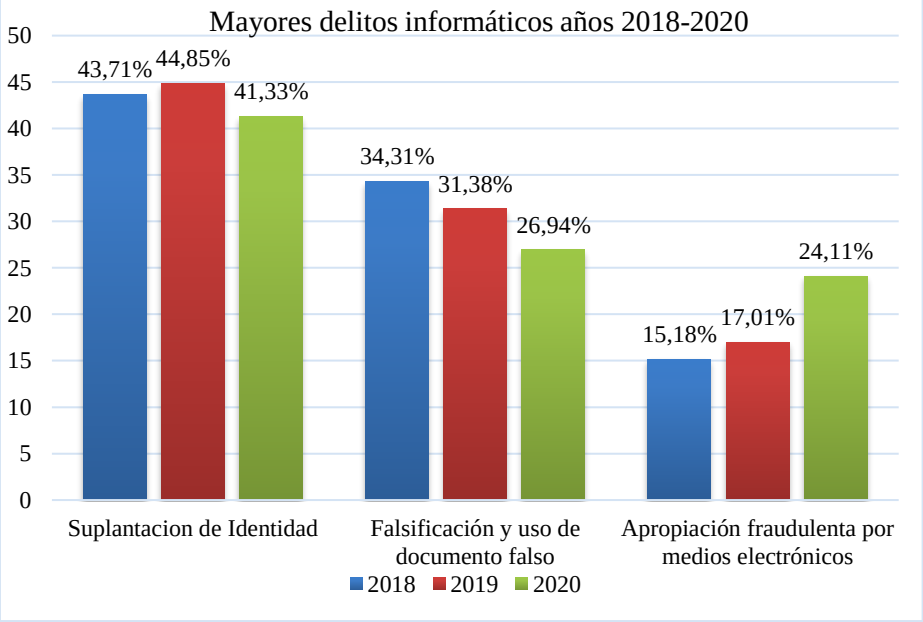


Fig. 4. Delitos informáticos con mayor número de denuncias 2018-2020

3.5 Generar una matriz del impacto tecnológico y financiero para prevención en las transacciones bancarias mediante normativas y estándares.

Para la generación de la matriz de impacto y frecuencia se definen dos escalas, la frecuencia, se establece una escala del 1 al 5, siendo 1 muy poco probable, 2 poco probable, 3 esperado, 4 frecuente y 5 muy frecuente. Para el impacto, se establece un factor de riesgo en una escala del 1 al 5, siendo 1 insignificante, 2 menor, 3 moderado, 4 alto y 5 catastrófico.

Por consiguiente, los datos de la tabla 9 se utilizarán para la matriz de impacto y frecuencia.

Table 9. Delitos informáticos según tipo 2014-2020

Años	Suplantación	Falsificación	Apropiación	Acceso no c.	Total delitos anual
2014	43,47%	33,57%	16,24%	1,79%	3122
2015	47,60%	31,52%	15,57%	1,72%	8242
2016	47,28%	35,35%	11,89%	1,65%	8792
2017	43,60%	37,77%	11,46%	2,59%	8427
2018	43,71%	34,31%	15,18%	2,49%	9560
2019	44,85%	31,38%	17,01%	2,39%	10264
2020	41,33%	26,94%	24,11%	3,14%	9529

Por otra parte, en la tabla 10 se muestran los cuatro delitos informáticos con mayor número de denuncias, los valores de impacto y frecuencia establecidos.

Table 10. Matriz de impacto y frecuencia

	Delito informático	Impacto	Frecuencia
A	Suplantación de identidad	4	5
B	Falsificación y uso de documento falso	4	4
C	Apropiación fraudulenta por medios electrónicos	3	3
D	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	2	1

Para finalizar, en la figura 5 se visualiza la ubicación de los delitos informáticos en la matriz de impacto y frecuencia. El delito de suplantación de identidad obtiene un impacto de 4(alto) y una frecuencia de 5(muy frecuente) porque según la tabla 4 el porcentaje se ha mantenido por arriba del 40% en los últimos 6 años y el impacto es alto porque si se suplanta la identidad se puede sustraer los datos y utilizarlos principalmente para el robo de dinero de cuentas bancarias.

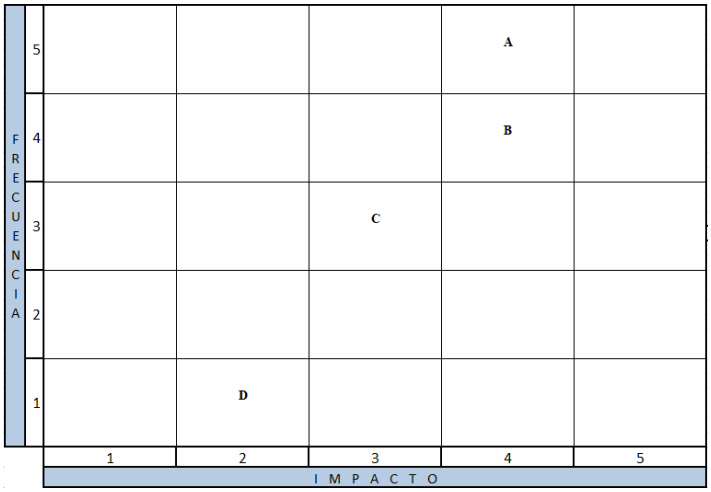


Fig. 5. Matriz impacto y frecuencia delitos informáticos

3.6 Contrastar las principales estrategias y técnicas de prevención de riesgos tecnológicos con reportes antiphishing

En una campaña de phishing se envían correos maliciosos a los usuarios para obtener las credenciales de usuario y contraseña. Para mitigar los ataques se utilizan técnicas de detección, estas abarcan programas de concientización, software de clasificación y técnicas que utilizan los proveedores de servicios. Es importante tomar en cuenta que para mejorar la detección de las campañas de phishing es posible realizarlo aprendiendo de experiencias anteriores, lo que puede ser ejecutado por un usuario o software con algoritmos de machine learning.

Las técnicas están categorizadas de la siguiente manera:

- Enfoque de detección: consiste en dos formas, la primera es el entrenamiento del usuario, se lo educa en lo referente a los ataques de phishing, esto permite que pueda distinguir entre mensajes malignos y no malignos. La segunda forma es la clasificación por software, el software realiza la tarea de clasificar mensajes de phishing en vez del usuario, para reducir la brecha del error humano o la ignorancia del mismo.
- Enfoque defensa ofensiva: el objetivo es generar campañas de phishing que no sean válidas, esto se logra desbordando el sitio web malicioso con credenciales no válidas, de esta manera el atacante tendrá un tiempo complicado para encontrar las credenciales originales
- Enfoque de corrección: al detectarse la campaña se comienza con el proceso de corrección, esto se realiza dando de baja los recursos de phishing; se lo logra reportando los ataques a los proveedores de servicios.

Enfoque de prevención: dependiendo del contexto puede significar: prevención para evitar que los usuarios se conviertan en víctimas. En este enfoque se utilizan las técnicas de detección; prevención de los atacantes para comenzar campañas de phishing, consiste en demandas y sanciones legales para los atacantes por medio de los entes legales correspondientes [18].

De acuerdo con el reporte anual del 2020 del centro de quejas de delitos en internet (IC3), que es una división gubernamental del FBI (Buró federal de investigaciones), indica que los casos pertenecientes a phishing y sus variaciones en E.E.U.U. registran un total de 241342 víctimas, las pérdidas aproximadas en el 2020 son de $54,241,075.

El IC3 recomienda lo siguiente:

- Las compañías en la mayoría de los casos no se contactan para solicitar usuarios y contraseñas.
- No haga clic en ningún correo o mensaje de texto que no haya solicitado, revise el número de teléfono de la compañía y no el que está en el correo, puede llamar a la compañía y verificar si el mensaje es legítimo.
- Examinar detenidamente la dirección de correo, la dirección web y si está escrito de manera correcta.
- Ser precavido con las descargas de contenido. Nunca abra archivos adjuntos de alguien que no conoce y sea cauteloso de correos con archivos adjuntos reenviados a usted.

Configurar autentificación de dos o más factores en cualquier cuenta que lo permita y no deshabilitar esta opción [32].

4 Discusión

Según la revisión de las estadísticas, que se citan en este artículo, se puede visualizar el aumento de casos de phishing. Existe un total de 3938 casos en el año 2020, mientras que Colombia reporta un total de 1753 en el año 2020 [33] lo que indica que este delito, además de haber aumentado, es el principal y mayor que en Colombia.

También es necesario destacar que, dentro de los tres mayores delitos informáticos en el Ecuador, el phishing, es el principal, en el periodo del 2014-2020 de acuerdo con la información de la Fiscalía General del Estado, seguido de la falsificación/uso de documento falso y la apropiación fraudulenta por medios electrónicos.

Los recursos que se destinan a combatir el phishing no aparecen listados en las estadísticas correspondientes, tampoco hay un indicio de los efectos económicos y financieros del phishing como: la cuantificación de pérdidas en dólares de cada uno de los casos o un aproximado total por año ni tampoco la tasa de éxito de los casos resueltos. Es importante tener más información del perfil de los usuarios que son víctimas del phishing, rango de edad, tipo de sector público o privado donde ocurren los delitos para poder tener posibilidades de mayor detección y prevención de este delito informático.

5 Conclusiones

Según lo revisado y presentado es importante destacar que el Phishing se ha dinamizado en los últimos seis años (2014-2020) de acuerdo con las cifras estadísticas de la Fiscalía General del Estado, esto significa que de acuerdo con su crecimiento ya es uno de los delitos informáticos que más crece en el Ecuador. Esto evidencia la falta de soluciones concretas para mitigar su expansión.
De acuerdo con la matriz de impacto y frecuencia, el phishing tiene una frecuencia alta de alrededor de más del 40% anual y un impacto con un valor de 4 que lo establece como un riesgo alto, ya que con los datos del usuario se pueden cometer muchos actos ilícitos desde acceso a cuentas bancarias hasta robo de información sensible.

Según las estadísticas del phishing, en el período 2014-2020 en el país, no solo que ha crecido a un ritmo alto anualmente, sino que es el principal y más frecuente delito informático en el Ecuador. Así mismo, se evidencia la poca prevención para mitigar su expansión sin dejar de tomar en cuenta el resto de los delitos que siguen incrementándose cada año.

La mejor prevención es estar preparados, lo que se logra con la capacitación constante a los usuarios, las herramientas físicas y lógicas que deben existir en cada institución pública o privada, planes de acciones y contingencia actualizados y aplicadas con regularidad por lo menos una vez al año. Es necesario contar con financiamiento para ejecutar estas estrategias y realizar las consultorías correspondientes con las empresas especializadas en seguridad informática.

El phishing es una amenaza constante que no va a desaparecer, por lo tanto, las acciones que deben seguirse para estar preparados involucran mejoras en la legislación, dotar de más recursos a las áreas correspondientes, capacitaciones continuas a los usuarios del sector público y privado, campañas con lenguaje sencillo para todos los usuarios que navegan diariamente en el internet y hacerles comprender los riesgos existentes.

Además, hay distintos mecanismos que se utilizan en phishing, que van innovándose y variando sus técnicas como, por ejemplo, el uso de códigos QR en correos fraudulentos, correos que solicitan el pago de pequeñas tarifas de centavos de dólares que después serán debitados con valores mayores, la tendencia al teletrabajo y problemas de seguridad en aplicaciones como Zoom donde las contraseñas se venden en la dark web o instaladores de la aplicación con malware. Todo esto debe ser informado y concientizado permanentemente ya que son pocos criminales los necesarios para realizar estos delitos y muchos los usuarios afectados.

La detección y prevención del phishing es fundamental para reducir el impacto económico y financiero como es la afectación del patrimonio y los ingresos de los usuarios, así como la reducción de la confianza en la realización de transacciones en los canales electrónicos que a su vez causan un efecto negativo en la actividad económica y financiera, así como el desincentivo que genera en los usuarios el uso de los canales electrónicos.

Las estadísticas referentes a los delitos informáticos deberían estar en una sección propia dentro del sitio web de la Fiscalía General del Estado, a la fecha actual (mayo de 2021) en el enlace de estadísticas solo están las categorías: violencia de género,

robos y fuerza de tarea. Dentro de la categoría robos no aparece lo referente a los delitos informáticos ni tampoco se tiene una cuantificación de los valores monetarios en dólares sobre las pérdidas ocasionadas, esto podría ser un trabajo de investigación posterior. Además, deberían coordinar en la prevención y mitigación del delito la Superintendencia de Bancos y la de Economía Popular y Solidaria, que son organismos de supervisión.

Referencias

1. Pranggono, B., Arabo, A.: COVID -19 pandemic cybersecurity issues . Internet Technol. Lett. 4, e247 (2021). https://doi.org/10.1002/itl2.247.
2. Plachkinova, M.: Exploring the Shift from Physical to Cybercrime at the Onset of the COVID-19 Pandemic. Int. J. Cyber Forensics Adv. Threat Investig. 2, 50–62 (2021). https://doi.org/10.46386/ijcfati.v2i1.29.
3. Bitaab, M., Cho, H., Oest, A., Zhang, P., Sun, Z., Pourmohamad, R., Kim, D., Bao, T., Wang, R., Shoshitaishvili, Y., Doupé, A., Ahn, G.-J.: Scam Pandemic: How Attackers Exploit Public Fear through Phishing. (2021).
4. Veerasamy, N.: Cyber threats focusing on Covid-19 outbreak. 16th Int. Conf. Cyber Warf. Secur. 391 (2021).
5. Georgiadou, A., Mouzakitis, S., Askounis, D.: Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur. J. 1–20 (2021). https://doi.org/10.1057/s41284-021-00286-2.
6. Shammari, A. Al, Maiti, R.R., Hammer, B.: Organizational security policy and management during covid-19. In: Conference Proceedings - IEEE SOUTHEASTCON. Institute of Electrical and Electronics Engineers Inc. (2021). https://doi.org/10.1109/SoutheastCon45413.2021.9401907.
7. Al-Turkistani, H.F., Ali, H.: Enhancing Users' Wireless Network Cyber Security and Privacy Concerns during COVID-19. Presented at the May 11 (2021). https://doi.org/10.1109/caida51941.2021.9425085.
8. Stojnic, T., Vatsalan, D., Arachchilage, N.A.G.: Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. Secur. Priv. e165 (2021). https://doi.org/10.1002/spy2.165.
9. Llerena, J., Mendez, A., Sanchez, F.: Analysis of the Factors that Condition the Implementation of a Backhaul Transport Network in a Wireless ISP in an Unlicensed 5 GHz Band, in the Los Tubos Sector of the Durán Canton. In: 2019 International Conference on Information Systems and Computer Science (INCISCOS). pp. 15–22. IEEE (2019). https://doi.org/10.1109/INCISCOS49368.2019.00012.
10. Interpol: INTERPOL warns of organized crime threat to COVID-19 vaccines, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19%0Ahttps://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines.

11. Bou Sleiman, M., Gerdemann, S.: Covid-19: a catalyst for cybercrime? Int. Cybersecurity Law Rev. 2, 37–45 (2021). https://doi.org/10.1365/s43439-021-00024-9.
12. Ferreira, A., Cruz-Correia, R.: COVID-19 and Cybersecurity: Finally, an Opportunity to Disrupt? JMIRx Med. 2, e21069 (2021). https://doi.org/10.2196/21069.
13. Georgiadou, A., Mouzakitis, S., Bounas, K., Askounis, D.: A Cyber-Security Culture Framework for Assessing Organization Readiness. J. Comput. Inf. Syst. (2020). https://doi.org/10.1080/08874417.2020.1845583.
14. Muthuppalaniappan, M., Stevenson, K.: Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int. J. Qual. Heal. care J. Int. Soc. Qual. Heal. Care. 33, 1–4 (2021). https://doi.org/10.1093/intqhc/mzaa117.
15. Derecho Ecuador - CÓDIGO ORGÁNICO INTEGRAL PENAL, https://www.derechoecuador.com/codigo-organico-integral-penal.
16. Ochoa Marcillo, A.C.: Desafíos globales del cibercrimen: caso Ecuador período 2014–2019, https://repositorio.uasb.edu.ec/handle/10644/7919, (2021).
17. Quilligana Barraquel, J.E.: Elaboración de un proyecto de Ley de Defensa Cibernética, basado en la política de defensa nacional. (2021).
18. Khonji, M., Iraqi, Y., Jones, A.: Phishing detection: A literature survey, (2013). https://doi.org/10.1109/SURV.2013.032213.00009.
19. Bada, M., Nurse, J.R.C.: Profiling the Cybercriminal: A Systematic Review of Research. (2021).
20. Arshad, A., Rehman, A.U., Javaid, S., Ali, T.M., Sheikh, J.A., Azeem, M.: A Systematic Literature Review on Phishing and Anti-Phishing Techniques. Pakistan J. Eng. Technol. 4, 163–168 (2021).
21. Wen, H., Fang, J., Wu, J., Zheng, Z.: Transaction-based Hidden Strategies Against General Phishing Detection Framework on Ethereum. Presented at the April 27 (2021). https://doi.org/10.1109/iscas51556.2021.9401091.
22. Ivanov, M.A., Kliuchnikova, B. V., Chugunkov, I. V., Plaksina, A.M.: Phishing Attacks and Protection against Them. In: Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021. pp. 425–428. Institute of Electrical and Electronics Engineers Inc. (2021). https://doi.org/10.1109/ElConRus51938.2021.9396693.
23. Atmojo, Y.P., Susila, I.M.D., Hilmi, M.R., Rini, E.S., Yuningsih, L., Hostiadi, D.P.: A New Approach for Spear phishing Detection. Presented at the May 17 (2021). https://doi.org/10.1109/eiconcit50028.2021.9431890.
24. Hijji, M., Alam, G.: A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions. IEEE Access. 9, 7152–7169 (2021). https://doi.org/10.1109/ACCESS.2020.3048839.
25. Boukari, B.E., Ravi, A., Msahli, M.: Machine Learning Detection for SMiShing Frauds. Presented at the March 11 (2021).

https://doi.org/10.1109/ccnc49032.2021.9369640.
26. Gajera, K., Jangid, M., Mehta, P., Mittal, J.: A Novel Approach to Detect Phishing Attack Using Artificial Neural Networks Combined with Pharming Detection. In: Proceedings of the 3rd International Conference on Electronics and Communication and Aerospace Technology, ICECA 2019. pp. 196–200. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/ICECA.2019.8822053.
27. Ismail, S., Alkawaz, M.H., Kumar, A.E.: Quick Response Code Validation and Phishing Detection Tool. In: 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). pp. 261–266. IEEE (2021). https://doi.org/10.1109/ISCAIE51753.2021.9431807.
28. Khraisat, A., Alazab, A.: A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity. 4, 1–27 (2021). https://doi.org/10.1186/s42400-021-00077-7.
29. Abiodun, O.I., Abiodun, E.O., Alawida, M., Alkhawaldeh, R.S., Arshad, H.: A Review on the Security of the Internet of Things: Challenges and Solutions, (2021). https://doi.org/10.1007/s11277-021-08348-9.
30. Rahman, M.S., Halder, S., Uddin, M.A., Acharjee, U.K.: An efficient hybrid system for anomaly detection in social networks. Cybersecurity. 4, 1–11 (2021). https://doi.org/10.1186/s42400-021-00074-w.
31. Petersen, Kai & Feldt, Robert & Mujtaba, Shahid & Mattsson, M.: Systematic mapping studies in software engineering | Proceedings of the 12th international conference on Evaluation and Assessment in Software Engineering.
32. Internet Crime Complaint Center: FBI: Internet Crime Report 2020. Comput. Fraud Secur. 2021, 4 (2021). https://doi.org/10.1016/S1361-3723(21)00038-5.
33. Frasson-Quenoz, F., González, C.A.N.: Colombia's cybersecurity predicament. In: Routledge Companion to Global Cyber-Security Strategy. pp. 494–503. Routledge (2020). https://doi.org/10.4324/9780429399718-42.