UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE DERECHO

ESCUELA DE DERECHO

Medidas de seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phishing en el sistema financiero

TESIS PARA OPTAR EL TÍTULO DE

ABOGADO

AUTOR

Hillari Itati Lopez Ocampo

ASESOR

Victor Javier Sanchez Seclen

https://orcid.org/0000-0002-3953-5526

Chiclayo, 2023

Medidas de seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phishing en el sistema financiero

PRESENTADA POR

Hillari Itati Lopez Ocampo

A la Facultad de Derecho de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de

ABOGADO

APROBADA POR

Manuel Francisco Porro Rivadeneira
PRESIDENTE

Igor Eduardo Zapata Velez
SECRETARIO

Victor Javier Sanchez Seclen
VOCAL

Dedicatoria

A Dios, por su inmensa misericordia, bendición y protección cada día.
A mi padre David y mi madre María Isabel por su amor infinito, sus sabios consejos, valentía y apoyo incondicional.
A mi hermano Jack, por motivarme y alentarme.

Agradecimientos

Agradezco a Dios por sus infinitas bondades en mi vida. A mis padres, por el esfuerzo realizado para culminar esta primera etapa en mi vida profesional. A mi hermano, por su alegría y a toda mi familia que nunca dejó de confiar en mí. A mi asesor Víctor Sánchez Seclen, por guiarme con paciencia y bondad durante el desarrollo de esta investigación y al Dr. Manuel Francisco Porro Rivadeneira por sus conocimientos impartidos en el desarrollo de este trabajo.

Medidas de seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phishing en el sistema financiero

INFORME DE ORIGINALIDAD

23%	22%	4%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	2%
2	tesis.usat.edu.pe Fuente de Internet	2%
3	revoredo.pe Fuente de Internet	1%
4	hdl.handle.net Fuente de Internet	1%
5	repositorio.ucp.edu.pe Fuente de Internet	1%
6	repository.unad.edu.co Fuente de Internet	1%
7	www.sbs.gob.pe Fuente de Internet	1%
8	revistas.uteq.edu.ec Fuente de Internet	1%

Índice

Resumen **6**

Abstract **7**

Introducción **8**

Revisión de literatura **11**

Materiales y métodos **20**

Resultados y discusión **21**

Conclusiones **32**

Recomendaciones **32**

Referencias **33**

Resumen

El presente trabajo tiene como objetivo proponer medidas de seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phishing en el sistema financiero, utilizando la metodología cualitativa, sirviéndose de la técnica de fichaje, análisis documental, la observación y los instrumentos utilizados fueron las fichas textuales y de resumen, la guía de análisis documental y la guía de observación. Entre los resultados se obtuvo mediante un exhaustivo análisis las implicancias del phishing en el sistema financiero y patrimonio de los consumidores. Asimismo, es necesario argumentar mecanismos de protección que debe adoptar el sistema financiero para evitar afectación a los consumidores frente al phishing. Se concluye que, si todos los consumidores buscan proteger su patrimonio, entonces las medidas de seguridad bancarias para mitigar la vulneración de derechos de los consumidores frente al phishing que el legislador peruano deberá regular son; el respeto a los dispositivos legales del derecho patrimonial al consumidor, para ello, generar mecanismos de seguridad preventivos para evitar el phishing.

Palabras claves: fraude electrónico, sistema financiero, phishing, derecho al consumidor.

Abstract

The purpose of this work is to propose banking security measures to mitigate the violation of users' rights in the face of phishing in the financial system, using the qualitative methodology, using the technique of file filing, documentary analysis, observation and the instruments used were the textual and summary files, the documentary analysis guide and the observation guide. Among the results were obtained through an exhaustive analysis of the implications of phishing in the financial system and consumers' assets. Likewise, it is necessary to argue protection mechanisms that the financial system should adopt to avoid affecting consumers in the face of phishing. It is concluded that, if all consumers seek to protect their assets, then the banking security measures to mitigate the violation of consumer rights against phishing that the Peruvian legislator should regulate are: respect for the legal provisions of the consumer's property rights, to do so, generate preventive security mechanisms to avoid phishing.

Keywords: electronic fraud, financial system, phishing, consumer rights.

Introducción

Durante estos últimos años y por el avance de la tecnología nuestra sociedad ha evolucionado a pasos agigantados gracias a ello existe un aumento progresivo de información, de tal modo, los individuos han intervenido en el desarrollo tecnológicos, es por ello que, al ingresar a una plataforma virtual con dar un clic, se consigue la información deseada. Asimismo, el uso de la tecnología ha generado fraudes en el ámbito financiero, entre los cuales encontramos al phishing definido como un procedimiento empleado para despojar información y adquirir beneficios económicos.

En el ámbito internacional, en Colombia, el gremio representativo Asobancaria (2019), señala al phishing como la modalidad de fraude, que envía de manera masiva mensajes electrónicos apareciendo una dirección web falsa clonada de una entidad bancaria con el objetivo de obtener información de los consumidores como claves de acceso, etc.

Asimismo, en Colombia, en la revista escrita por Medina, Cárdenas y Mejía (2021) reveló que los ciberdelitos han ocasionado 31.498 denuncias. Los tipos de industrias más afectadas por este delito fueron: el financiero con un 40%, telecomunicaciones con un 26%, Gubernamental con 16%, productos con un 10% y la industria energética con una tasa del 9%. Con todo lo mencionado, el phishing se encuentra el primer lugar en el país.

Además, en México, Huerta citando a Panda (2021) mencionó que este fraude es una técnica de ingeniería social que radica en enviar correos electrónicos simulados cuya apariencia es engañosa, simulando que el usuario ingresa al sitio web correcto. De igual manera, la revista Profeco de México (2021) tiene herramientas que exhorta a los consumidores examinar los sitios de venta en línea; ya que durante los meses del 2019 se rastreó un total de 1,461 quejas por negocios en línea, además se realizaron conciliaciones del 74% con un promedio.

Por consiguiente, en Ecuador, para Benavides, Fuertes y Sánchez (2020) mediante la revista de Ciencias Informáticas, advirtieron diversas metodologías para impedir ataques de phishing, entre los más habituales encontramos; al correo phishing y por una página web; por lo general se informa a las víctimas que han obtenido un premio, a cambio del cual deben ingresar sus datos personales, otra técnica es, la página web falsificada, idéntica a la legítima.

Del mismo modo, en Argentina, en el diario de la Universidad Nacional de la Plata, (2020) se señalaron otras características basadas en albergar información mediante un mensaje SMS en su teléfono o una comunicación automática y hasta llamada telefónica del usuario, en aquella se tima a los consumidores infringiendo ser la organización confiable y solicitando información personal, posterior a ello engañando y utilizando esa data sin autorización del consumidor.

En consecuencia, la Organización de los Estados Americanos (2018) señaló que las entidades bancarias obtuvieron ascendentes índices de digitalización, generando un aumento de usuarios en la banca electrónica, además, de efectuar servicios por internet o pagos a través de dispositivos móviles, que pretenden obtener ventajas de las tecnologías, sin embargo, existen peligros que corresponden prevenir con el resultado de atenuar los potenciales ataques y escenarios de fraude expuestos a empresas y usuarios.

A nivel nacional, en Lima, Flores, y otros (2020), señalaron otra particularidad de ataque a empresas: un 29% de casos se origina al emplear malware, además el phishing alcanza un 24% y un 7% utilizando el escaneo en red.

Para Aroni y Barrios (2018) citando el portal de la SBS el sistema financiero en el Perú está estructurado por 54 empresas entre entes financieros y otras compañías e instituciones adecuadamente reglamentadas, encargadas de realizar operaciones múltiples, del mismo modo, gozan de bienes valorizados por 404 millones de soles. Estas empresas realizan una creciente economía y tiene por objetivo regularizar el dinero de quienes desean ahorrar hacia los inversionistas. En resumen, las entidades realizan esta función son denominadas intermediarios o mercados financieros.

Por lo tanto, ampliaremos medidas de seguridad apropiadas para advertir y reducir la cantidad de fraudes, añadiendo estrategias de navegación tangibles para los consumidores a fin conocer cuando son víctimas de agresiones de phishing fundados en políticas de seguridad permitiendo a los usuarios verificar de manera automática el sitio web al que se encuentran conectados. Es por ello que, se ha formulado el siguiente problema ¿Cuáles deberán ser las medidas de seguridad bancarias para mitigar la transgresión de derechos de los usuarios frente al phising en el sistema financiero peruano?.

En efecto, mediante esta tesis se buscan implementar estrategias orientadas a la concientización de consumidores frente al phishing, y obtener su información en un dispositivo digital, debido al incremento de ataques a la banca electrónica ejecutados a través de internet, los cuales vulneran la probidad y confiabilidad de datos y patrimonio de la entidad bancaria, además de la confianza consignada por el usuario de la cuenta de seguridad del sistema financiero para realizar las diversas transacciones bancarias mediante plataformas virtuales.

Ahora bien, el aporte práctico de este tópico de investigación a desarrollar, radica en las entidades bancarias y financieras, que buscan brindar una adecuada seguridad para evitar la vulneración de derechos, por lo cual, deben proveer información sobre características, detalles y tipologías que presenta el phising. Por lo tanto, al presentarse este fraude la entidad bancaria deberá solucionar de manera inmediata los peligros que atraviesa el consumidor al utilizar 10

herramientas informáticas, agregando, que estas dificultades traen como consecuencia tras la ineficaz actuación.

En cuanto al aporte metodológico, el trayecto es cualitativo, mediante un análisis teórico y legal con los resultados obtenidos, plantearemos una propuesta de implementación normativa de seguridad bancarias para mitigar la transgresión de derechos frente al phishing en el sistema financiero, debido que, las entidades bancarias han entregado facultades a diversos mecanismos cibernéticos para que los usuarios realicen sus operaciones bancarias, adoptando un menor compromiso por parte de la empresa referido al área de atención al cliente reemplazados por servicios ofrecidos en una página web.

Del mismo modo, consideramos de vital importancia tutelar los derechos fundamentales de todos los consumidores, además, beneficiar con medidas oportunas y rápidas tras ser víctimas del phishing. En base a ello, podrán permitir el ejercicio adecuado de seguridad y gozarán de los beneficios y mejoras en las condiciones de ventaja que se obtengan como producto de una correcta y eficiencia actuación de las entidades financieras.

A partir de lo dicho, el presente estudio, tiene como objetivo general recomendar medidas de seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phishing en el sistema financiero peruano. Los objetivos específicos son: analizar las implicancias del phishing en el sistema financiero respecto al derechos de los usuarios e identificar mecanismos de protección que debe adoptar el sistema financiero para evitar afectación a los usuarios frente al phishing.

Ante ello, se formuló la hipótesis de trabajo: Si todas las entidades bancarias buscan proteger el patrimonio de los usuarios entonces deberán establecer estándares de seguridad adecuados para mitigar la vulneración de derechos de los usuarios frente al phising en el sistema financiero como: generar mecanismos cibernéticos preventivos para evitar el phishing e implementar el deber de información del banco.

Asimismo, el aporte permitirá buscar un régimen de protección del patrimonio de los consumidores, generando medidas de seguridad tanto para los clientes como para las entidades bancarias debido a la importante información que contienen nuestros dispositivos electrónicos, del mismo modo, debe existir de una adecuada gestión sobre nuestros datos por el almacenamiento de dinero, los cuales son muy atractivos para los defraudadores, generando un incremento en los ataques cibernéticos.

Revisión de literatura

En cuanto a los antecedentes de estudio, se inició revisando distintas tesis de pre-grado, maestría, libros, revistas y artículos científicos, los cuales conciernen al trabajo de investigación, para alcanzar los objetivos formulados.

1.1 ANTECEDENTES

1.1.1 Investigaciones internacionales

En el ámbito internacional, el autor Hernández y Mendoza (2018), en su proyecto de pregrado "El funcionamiento del comercio electrónico, categorías seguridad para usuarios y demografía de usos habituales". Los autores tienen como objetivo conocer las plataformas web utilizadas en el comercio electrónico, informar a usuarios de internet sobre las distintas formas de seguridad a través de una ejemplificación demográfica actual.

Los autores mediante su investigación exponen la problemática de muchas empresas pequeñas y grandes las cuales han empleado medios tecnológicos para sus negocios, sin embargo, la desinformación de los usuarios al adquirir un bien o servicio es una desventaja para quienes desean ahorrar tiempo y dinero, asimismo, los proveedores son afectados por carecer de confianza de sus clientes. En consecuencia, el comercio electrónico en México no existe una cultura informática en comparación de los países desarrollados.

Dado que, esta investigación es transcendental para el estudio debemos señalar que los negocios virtuales demandan revoluciones de marketing porque estudia numerosas plataformas que existen para mercantilizar, que son utilizadas cotidianamente por miles de usuarios. En México al igual que en muchos países latinoamericanos no poseen educación y/o información para evitar los problemas de internet, como la seguridad consecuencia al nulo conocimiento de ello.

Aguirre, (2022), en su artículo titulado "Ciberseguridad, desafío para México y trabajo legislativo", presentado en la Academia Belisario Domínguez de la Ciudad de México, es gran ayuda para confrontar otros delitos como por ejemplo fuga de datos personales, infracción de privacidad, estafas, flujos financieros ilícitos, entre otros. Conviene subrayar que, los gobiernos de diversos órdenes tienen interés en proteger la seguridad nacional, por ello, deben aplicar políticas públicas para proteger el patrimonio de la sociedad.

Siendo así, menciona mecanismos para custodiar la información en medios digitales, además explica como reconocer los riesgos y establecer factores de estabilidad, estos ataques generan daños a familias y empresas, por lo que debido a la falta de actualización de los equipos, el uso de programas no originales y la falta de modernización en el software utilizado por empresas bancarias generan vulnerabilidad. Se debe agregar que la prevención y educación son

fundamentales para evitar riesgos, asimismo implementar políticas públicas y marco normativo para combatir el peligro.

Por su parte, el autor Zabala, (2021) en su artículo titulado "Responsabilidad bancaria frente al delito de phishing en Colombia", presentado y publicado ante la Revista Creative Commons nos sirve porque trata sobre la responsabilidad del banco en Colombia, además, justifica el minucioso tratamiento que debe preexistir, de tal manera que permita identificar vacíos jurídicos en la relación banco – cliente.

Además de ello, admite fortificar la representación del banco al colocar un portal virtual que contribuya a su dinamismo para su diligencia ante los clientes de manera segura en la relación contractual, también reducir pérdidas y daños para el cliente, sobre todo señala que, el banco al poseer un enfoque privilegiado debe asumir la responsabilidad y resarcir daños, en cambio, el cliente entrega confianza y seguridad.

Para Castillo (2021) en su tesis de maestría titulada "Phishing: día de pesca", presentada ante la Universidad Externado de Colombia. El autor tiene como objetivo analizar el procedimiento de enjuiciamiento delictivo colombiano instaurado como dispositivo reactivo a fin de atender sucesos informáticos en particular el phishing, instituyendo y creando insumos distinguidos para acoger nuevas medidas. Para así concluir, aportando conocimiento e impedir que en el medio digital existan víctimas de acciones de la cibercriminalidad.

Dicho lo anterior, se conoce que, el Derecho Penal es utilizado como última ratio, sin embargo, al no constituirse otras alternativas ante esta conducta se establecieron andamiaje judicial, herramientas sofisticadas como software y hardware que permitirán ejecutar óptimas destrezas por la comunidad científica y acumular sus esfuerzos en aquellas.

Santos, (2021), en su tesis de pregrado titulada "Aspectos técnicos del delito de phishing vinculados a los elementos del ordenamiento jurídico" presentada ante la Universidad de León, su trabajo tiene como finalidad adaptar técnicas para evitar el delito de estafa informática mediante las TICs.

Tras la pandemia se incrementaron los delitos informáticos como el phishing, hacking, cracking, childgrooming entre otros, por tanto, se deben elaborar estrategias penales que adecuen su normativa al raudo cambio que atravesamos. Bajo este contexto, la navegación en la web y mecanismos virtuales les corresponderían una criptología nacional máxima.

1.1.2 Investigaciones nacionales

Mengoa (2021) en el presente análisis para elegir el título de abogado: "Punibilidad del phisher-mule en el fraude informático en Perú", presentado en la Universidad César Vallejo. Tiene como finalidad determinar el comportamiento del phisher-mule en los delitos

informáticos en el Perú. La autora llega a la siguiente conclusión: en el Perú, se castiga el acceso ilícito en el sistema informático, pero no existe un procedimiento claro del delito de estafa informática, encapsulado en el artículo 196-A, numeral 5 del Código Penal, señalado como estafa agravada, el cual tiene un resultado interesante, más aún si la infracción involucra otras conductas criminales como el phisher- mule, que favorece rápidamente en la consumación del acto delictivo y del daño al patrimonio.

Ahora bien, la presente tesis nos permite fundamentar la necesidad de actuación para un cooperador al ejecutar y materializar el hecho delictivo, sin embargo, nuestro sistema actual penal peruano vislumbra algunos conflictos para advertir, neutralizar y sancionar los delitos informáticos en nuestro ámbito nacional, entre los cuales encontramos la identificación física, el deterioro del patrimonio de personas naturales y la dificultad para remediar el daño ocasionado por entes externos, la disolución de la responsabilidad penal de organizaciones estructuradas.

Ananías, (2020) en su Trabajo Académico para optar el título de abogado: "Análisis comparativo del phishing y responsabilidad civil de los banco, previa y posterior a la entrada en vigencia de la Ley 21.234", presentado en la Universidad del Desarrollo, para optar al grado académico de Magíster en Derecho de Empresa, tiene como objetivo demostrar la diferencia y definición de los fraudes más recurrentes, además de la responsabilidad que tienen las entidades bancarias en la creación de los sistemas informáticos, asimismo, el resguardo respecto a los fondos depositados. El autor concluye: con un significativo cambio legislativo previo a la entrada en vigencia de la Ley 21.234, evaluando los cambios que ocasionan vulnerabilidad al sistema financiero.

Esta investigación nos servirá para implantar políticas de seguridad al utilizar los medios tecnológicos que buscan establecer principios básicos, además de instituir la confidencia ineludible en la utilización de la administración electrónica, indemnizar, crear circunstancias óptimas para utilizar mecanismos electrónicos y garantizar la seguridad de los sistemas.

Trejo, (2019) en su Trabajo Académico para optar el título de abogado: "Identificación del phishing como figura penal relevante en su incidencia con la seguridad de los usuarios afiliados a la banca por internet", presentado en la Universidad Nacional José Faustino Sanchez Carrión de Huacho, su propósito es comprobar vacíos legales en el Nuevo Código Procesal Penal Peruano y leyes complementarias en delitos informáticos. El autor llega a la siguiente 14 conclusión: Una inadecuada información o carencia de esta puede ocasionar grandes peligros para los consumidores y el phishing a nivel mundial es uno de los delitos más comunes de internet el cual de manera genérica utiliza el spam.

Por lo tanto, esta tesis nos ayudar a conocer sobre los negocios por internet y cuales han generado incomparables comodidades para los usuarios, sin embargo, su errónea aplicación generaría pérdidas a las entidades bancarias y a los consumidores, por ello debemos buscar preservar e informarnos, asimismo, las entidades bancarias también deben doblar refuerzos.

Campos (2018) en su Artículo científico: "La responsabilidad civil de los bancos por el riesgo de phishing", presentado en la Universidad Mayor de San Marcos. El autor indica que el desarrollo tecnológico y los nuevos servicios que operan en el ciberespacio han traído consigo nuevos riesgos, para ello los bancos vienen reforzando sus medidas de seguridad para evitarlos. Además, se pretende fijar la responsabilidad de los bancos, con la finalidad de cumplir con su rol vigilante, enfocando su atención en la gestión de riesgos, asumiendo una conducta diligente frente a los usuarios.

Esta investigación nos ayudará a analizar los beneficios que otorgar los mecanismos electrónicos de las entidades bancarias, para ejercer una actuación de los ámbitos bancarios es necesario dilucidar que la banca por virtual se hace responsable sobre algunos fraudes, pero el punto de partida no radica en ello, por el contrario, la interrogante se suscita que si las medidas que establecen las entidades bancarias son suficientes para los consumidores.

Chavez, (2018) en el presente trabajo para conseguir el título de abogado: "El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de lima norte, 2017", presentado en la Universidad Federico Villareal. Tiene como objetivo establecer la relación entre el delito de sistemas informáticos y los derechos a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017. Actualmente la tecnología, es un mecanismo que comunicación muy manejada en nuestra vida cotidiana, no obstante, carece de instrumentos correctos en su uso siendo este motivo base por el cual se afectan derechos fundamentales, esta problemática motivó su estudio.

Podemos decir que, los delitos financieros no se han tratado de manera adecuada en nuestro sistema financiero, sin embargo, en el sistema penal obtienen una tratativa drástica, pero no es suficiente debido a la vulneración de los derechos de los usuarios.

1.2 BASES TEÓRICAS

El auge de la transformación tecnología experimenta grandes cambios en nuestro sistema financiero, no solo en las entidades bancarias, sino también en las diversas industrias, es por ello, que el inicio de esta figura corresponde a los ataques de los hackers en la plataforma de entidades bancarias, las cuales modifican la estructura generando confusión a los usuarios al ingresar al sitio web erróneo, el objetivo es conseguir la confianza de la víctima y para sustraer sus cuentas bancarias de usuarios; los cuales entregan una serie de razones plausible o

incentivos idóneos en el orden a que el receptor para formar la convicción de un mensaje verdadero y, por ende, entregar sus datos sin reservar. (Flores Cáceres, 2017, pág. 7)

1.2.1 Definición del phishing

El phishing o suplantación de identidad es un procedimiento empleado por ciberdelincuentes quienes obtienen información de los usuarios de manera fraudulenta. Su frecuente uso es a través de redes sociales en específico el correo electrónico, por el cual se obtiene información detalla de los usuarios quieres a través de un cuestionario, encuesta o formulario de una forma muy sencilla. Es preciso mencionar que este tipo de prácticas son considerados delitos informáticos debido a su obtención de datos los cuales coadyuvan para la ejecución de actividades ilícitas. (Giraldo y Duarte, 2018, p.33)

Esta particularidad de simulación electrónica, que adquiere identificaciones personales de forma engañosa. El phisher o embaucador se suplanta identidad de una compañía de confianza y a través del envío de un mensaje electrónico o a la falsificación de la página web generando desconcierto al beneficiario y consigue información como el número de la tarjeta y clave secreta.

Simultáneamente, el correo demuestra diversas evidencias como, el reajuste de datos porque la cuenta será deshabilitada por precaución o indicando que el usuario ha sido beneficiario de una recompensa e incitando a confirmar su abono o recompensa, finalmente digitado el número de cuenta y clave secreta esta es acumulada y utilizada para suplantar al cliente, efectuando compras, transferencias de su dinero o ingresar a su correo electrónico personal. (Defensor del cliente financiero, 2008)

Asimismo, para la Superintendencia de Banca y Seguros (2019) menciona que el phishing es una modalidad de robo que opera a través del envío de un correo electrónico y reemplaza la imagen de una empresa o entidad formal (adaptando el uso de los colores y logotipo de las compañías) con la finalidad de adquirir datos para utilizarlos de forma fraudulenta. (p.05)

Con lo ya mencionado, se debe señalar que las operaciones realizadas mediante el comercio electrónico y las transacciones relacionadas a estas generan un gran desvanecimiento en nuestra seguridad jurídica a pesar de travesear un rol muy importante como son las relaciones bancarias, pago de servicios, compra de acciones o pago de proveedores, son originadas por compras por internet y la confianza que instauramos en los escenarios virtuales de los bancos, sin duda se debe establecer garantías para salvaguardar el patrimonio del consumidor.

1.2.2 Clases de phishing

1.2.2.1 Phishing clonado

El auge de la transformación tecnología experimenta grandes cambios en nuestro sistema financiero, no solo en las entidades bancarias, sino también en las diversas industrias, es por ello, que el inicio de esta figura corresponde a los ataques de los hackers en la plataforma de entidades bancarias, las cuales modifican la estructura generando a los usuarios la confusión de ingresar al sitio web adecuado. En palabras de Kenet (2021) este artificio cibernético es el mecanismo más utilizado conocido como phishing tradicional para sustraer información suplantando o clonado páginas web legítimas en las cuales los usuarios brindan datos confidenciales, con este tipo de engaño se obtienen mensajes al correo electrónico solicitando datos específicos como; contraseñas, números de cuenta o números de tarjetas, etc. Esta modalidad envía masivos emails para investigar el inicio de una entidad real como bancos, universidades, empresas, centros comerciales, etc. (pág. 59)

1.2.2.2 Phishing basado en páginas web o malware

Existe un sinfín de virus, troyanos y malware que ingresan al dispositivo informático, del mismo modo hay equipos que ya están contaminados originados por carencia de protección, configuradas para navegar en páginas simuladas con fácil acceso a internet sin poseer los cuidados requeridos al ingresar a numerosas plataformas y abrir correos electrónicos sospechosos, sin utilizar antivirus, etc.

Para Mariano (2020) se denomina malware por su redacción inglesa malicius software a cualquier otro arquetipo de lenguaje informático, que al ejecutarse realiza operaciones perjudiciales en un procedimiento de carácter internacional y sin el conocimiento del usuario o propietario de dicho sistema. La estructura del malware puede contener más de un componente, los cuales están destinadas a intercambiar mecánicamente la infección, ocultar la funcionalidad efectiva del malware y finalmente una porción destinada a ocultar la actividad maliciosa. (pág. 3)

Por lo tanto, radica en un mecanismo hostil, intrusivo que intenta irrumpir, destruir o deshabilitar, ordenadores, redes, dispositivos móviles para gestionar un control parcial de las operaciones de un dispositivo. “Esta modalidad consiste en recibir un correo conteniendo archivos adjuntos con un software malicioso indicando un link para descargar un archivo infectado”. (Rosero, 2021) En resumen, la finalidad del malware es sustraer dinero al usuario ilícitamente, sin destruir el hardware del equipo de red, eliminando datos, alterando cifras y secuestrando funciones elementales del computador para informar su diligencia en el ordenador sin su conocimiento o autorización.

1.2.3 Operatividad del phishing

Actualmente en nuestra vida cotidiana existe una extensa heterogeneidad de desconocidos fenómenos delictuosos y renovadas modalidades de comisión agresiones habituales, en específico a través de procedimientos o redes informáticas de transmisión e intercambio de datos, cuya complejidad operante obstaculiza su seguimiento y aumenta los niveles de impunidad.

En la revista Cisco Cybersecurity series (2019) se menciona que los ataques de correo electrónico más frecuentes es la suplantación de identidad en Office 365, el envío parece proceder de Microsoft argumentando que se suspenderá su dirección electrónica por errores o infracciones de la política, y la única condición para impedirlo es proporcionando el enlace suministrado. Se trata de un intento de usurpar sus credenciales, incluso los mensajes de correo electrónico y las URL manipuladas logran tener un aspecto similar, luego de pulsar sobre el enlace le trasladará a una página de inicio de sesión de aspecto oficial solicitando su información. (pág. 7)

Con lo antes mencionado, se evidencia un sitio web ficticio y con esta técnica es frecuente iniciar sesión mediante una cuenta de correo electrónico informal conteniendo otra URL, generando así ataques de identidad, dichas vulneraciones son usuales en la nube como Gmail y Outlook, dada la prevalencia de las cuentas y la forma de uso para acceder a distintos sitios web no resultaría extraño que los atacantes también hayan creado sitios de phishing en ese entorno.

1.2.4 Fases del phishing

1.2.4.1 Planificación y configuración:

Esta fase es equivalente a la distribución de individuo o un país. Con el propósito de extraer identificaciones de la víctima y la red, por lo cual se realizará un estudio de tráfico. Posterior a este reconocimiento, se establecen ataques mediante la dilatación de medios viables como el sitio web, correos electrónicos que contienen enlaces maliciosos, etc. Estas herramientas esencialmente redireccionan al usuario hacia una página web fraudulenta.

1.2.4.2 Ataque de Phishing:

Durante la segunda etapa se realiza la actividad real, los agresores remiten correos electrónicos falsificados a la víctima, empleando direcciones de correo electrónico recolectadas, requiriendo información sensible. Comúnmente los emails de phishing se encubren en páginas de organizaciones bancarias de buena reputación solicitando datos específicos de la víctima para actualizar sus registros, realizando preguntas que deben responder perentoriamente haciendo clic en algún enlace malicioso.

1.2.4.3 Ruptura/Infiltración:

Mediante esta fase la víctima al hacer clic en el enlace malicioso se instala automáticamente un malware en su dispositivo, permitiendo el acceso al sistema al atacante y consintiendo cambiar sus configuraciones y derechos de acceso. En otras situaciones al ejecutar clic en el enlace malicioso también consiguen que el usuario común sea re direccionado a páginas falsas.

1.2.4.4 Recopilación de datos:

Al ingresar los atacantes al sistema del usuario y extraer datos confidenciales de sus cuentas bancarias proporcionados en sitios web y páginas de dudosa procedencia, el atacante fácilmente conseguirá acceder a ella, y eventualmente trasladar esa información generando así pérdidas financieras. Asimismo, los ataques de malware consiguen acceso remoto al sistema del usuario y extraen los datos requeridos o realizan cualquier cambio según su voluntad.

1.2.4.5 Extracción:

Esta es la etapa concluyente del período. Posteriormente de adquirir el acceso y la indagación solicitada, se excluye toda la evidencia como las cuentas inexistentes del sitio web. Finalmente, se calcula el grado de éxito de su irrupción, para perfeccionar sus futuros ataques. **1.3 BASES CONCEPTUALES**

1.3.1 El phishing

En palabras de Paredes (2018) el phishing es una conducta que deriva del verbo fishing (pescar), el cual está referido al envío de e-mail empleando el nombre de la entidad bancaria, colocando un link y web falsa mediante el cual induce al usuario a brindar información confidencial sobre sus cuentas bancarias, tarjeta de crédito o su clave secreta. A través de diversos mecanismos ilícitos se realiza la creación de una página web falsa de una institución bancaria para hacer creer a los clientes que se trata de una operación bancaria segura con su banco. (p.14)

Para la Superintendencia de Banca y Seguros (2019) menciona que el phishing es una singular modalidad de estafa que utiliza el envío de un correo electrónico que reemplaza la imagen de una empresa o entidad formal (mediante el uso de los colores y logotipo de dicha empresa) con el objetivo de obtener datos como claves, cuentas bancarias, números de tarjeta de crédito, entre otros, para utilizarlos de forma fraudulenta. (p.05)

Con respecto a ello, el phishing inicia cuando el estafador suplanta la identidad de una organización de confianza del usuario, por ejemplo: el banco, empleando una falsa comunicación “oficial” electrónica, la cual buscará solicitar revelar su información secreta, como claves u otra información bancaria, dicha solicitud de información va acompañada de un sentido de urgencia o incluso de pánico como la amenaza de cierre de cuentas aspectos estos que motivan al usuario a acceder a la solicitud. (p. 146)

Para el caso en concreto el estafador persuade al cliente en proveerle los datos personales, cuando el consumidor contesta la comunicación electrónica o telefónica y le brinda su información, el consumidor pierde total control sobre su patrimonio, es por ello, que mi propuesta mediante el presente trabajo es salvaguardar e implementar mecanismos que protejan al usuario.

Por otro lado, la segunda modalidad, el estafador opera mediante la realización de una solicitud u encuesta y al colocar todos los datos, el correo de manera encriptada contiene un enlace que direcciona a un sitio web falso, sitio que resulta no igual, pero sí muy similar al oficial, por lo cual, al ingresar al sitio web el defraudador ya habrá capturado nuestra información y puede cumplir con su objetivo criminal.

1.3.2 Derecho de los usuarios

Los derechos de los usuarios forman parte de una nueva clase en derechos distintos a los personales y su defensa debe hacerse en forma grupal. El hecho de que el Derecho del Consumidor sea una disciplina relativamente nueva no quiere decir que el derecho anteriormente, no se haya preocupado por los consumidores. (p.153)

Nuestra legislación nacional según lo establecido en el Código de Protección y Defensa del Consumidor (Ley 29571), consideran que los consumidores, son todas las personas naturales o jurídicas que adquieren, utilizan o disfrutan como destinatarios finales productos o servicios materiales e inmateriales, en beneficio propio o de su grupo familiar o social, actuando así en un ámbito ajeno a una actividad empresarial o profesional. No se considera consumidor para efectos de este Código a quien adquiere, utiliza o disfruta de un producto o servicio normalmente destinado para los fines de su actividad como proveedor.

La Constitución Política del Perú en el Artículo 65°señala que; “El Estado defiende el interés de los consumidores y usuarios. Para tal efecto garantiza el derecho a la información sobre los bienes y servicios que se encuentran a su disposición en el mercado. Asimismo, vela, en particular, por la salud y la seguridad de la población”.

Para Schwalb (2020) la regulación del derecho al consumidor busca preservar la conmutabilidad y el balance entre las relaciones de consumo y los proveedores de bienes y servicios que realizan una actividad lucrativa, la autora señala, que el consumidor se encuentra en desventaja en relación con el conocimiento que se desea hacer uso para un óptimo consumo.

1.3.3 Sistema financiero

Durante algunos años nuestro sistema financiero atravesó una gran caída, por problemas políticos, una economía decreciente era una visión panorámica sobre nuestro patrimonio, poco se ha hablado del sistema financiero como principal canalizador de fondos excedentes de los

agentes superavitarios hacia aquellos usuarios con proyectos rentables y con recursos insuficientes para ponerlos en marcha. Por lo mencionado, el desarrollo del sistema bancario es crucial para el desarrollo de la economía y su competitividad. El sistema bancario es un componente importante del sistema financiero e incluso, en algunas economías como las de América Latina es el componente dominante.

En este sentido, la Superintendencia de Banca y Seguros (SBS) imprime que el principal objetivo del sistema financiero es buscar la estabilidad económica por lo cual, su reglamento es elemental en el diseño de un marco normativo riguroso y eficaz que inclusive ha logrado ser reconocido como un referido internacional. Los lineamientos de normas potestativas instauran una guía ventajosa, al mismo tiempo, la adaptación de estándares internacionales utilizados al tenor local, examina almacenar los riesgos presentes en la economía peruana. (pág.01)

De manera similar, el sistema financiero cumple un rol más amplio que la provisión de recursos, una vez que adopta practicas modernas, elevan la eficiencia y la productividad, y por ende el crecimiento económico. Por ejemplo, los positivos efectos para la productividad derivados del desarrollo del comercio electrónico o de la aplicación de las TIC y a ciertos servicios de la administración pública (como pago de impuestos, cobro de subsidios, entre otros) en los cuales el sistema financiero opera como interfaz entre el proveedor y el destinatario final.

Finalmente se puede mencionar que, el sistema financiero peruano cumple un papel fundamental en el progreso económico como lo han mencionado los autores, es por ello que, se puede observar una economía creciente y un sistema financiero en esa misma línea, sin embargo, aún existen deficiencias.

Materiales y métodos

La investigación desarrollada es de tipo documental, la cual se ha ejecutado bajo un minucioso análisis en la búsqueda, almacenamiento y procesamiento de información relacionada al problema; adquirida mediante artículos científicos, libros, revistas digitales académicas, páginas web, que ayudaron a moldear el objeto de estudio efectuado. Asimismo, la indagación surgió con la delimitación del problema, continuó con la selección y revisión rigurosa y sistemática del material bibliográfico, posterior a ello, la información fue constituida y sintetizada mediante la técnica del fichaje.

En adición, la investigación es de carácter cualitativo y en orden a los objetivos planteados, busca determinar las medidas preventivas que el sistema financiero debería adoptar frente al phishing a fin de cautelar el patrimonio de los consumidores. En orden a ello, este proyecto de tesis sustentará los criterios jurídicos por los que será necesario implementar medidas de

seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phising en el sistema financiero.

Por último, este artículo ha seguido con los lineamientos solicitados para una investigación bibliográfica, empleando el método analítico, paradigma interpretativo, recopilación y sección de documentos, por consiguiente, esta investigación se concretizó con aportes prácticos generados por el presente trabajo, asimismo, contribuyó de manera significativa en los mecanismos protectores del sistema financiero en el país.

Resultados y discusión

En este acápite abordamos las implicancias del phishing en el sistema financiero y patrimonio de los usuarios, asimismo, argumentamos mecanismos de protección que se deben adoptar para evitar afectación a los usuarios, finalmente, corresponde proponer medidas de seguridad bancarias para mitigar la vulneración de derechos.

3.1. Derecho de los usuarios en el phishing

3.1.1. Afectaciones al patrimonio del usuario

En la actualidad se han recibido cientos de denuncias por suplantación de identidad, entre los fraudes informáticos más investigados encontramos al phishing, cuya modalidad busca suplantar la identidad de una compañía bancaria o entidad financiera mediante creación de perfiles simulados para efectuar fraude, estafa u otros delitos.

En razón de ello, es importante determinar las afectaciones existentes al patrimonio del usuario logrando obtener datos confidenciales, en su mayoría tiene como finalidad adquirir beneficio económico, ocasionando suplantación de identidad, robo de dinero en bancos, vulneración a nuestra privacidad, es decir, utilizan cuentas robadas para fines delictivos.

- **Suplantación de identidad:** causado por otra persona que adquiere u obtiene información íntima de manera no consentida. Dicha operación es efectuada con fines fraudulentos o algún otro fin delictivo, asimismo, se obtiene rúbricas, número de tarjetas de crédito, identificación, datos explorados con el fin de consumar timos suplantando a la víctima, además, es sustraída con designios ilegales, por ejemplo; requerir préstamos, realizar adquirir en línea o instalar de los capitales financieros. (Barrantes Centurión, Sánchez Silva y Gutiérrez García, 2020)
- **Robo de dinero en bancos:** la sustracción se origina por el desfalco de identificación, cuando los delincuentes roban información íntima recogida en las cuentas. Con las cuentas y datos sustraídos, los hackers consiguen comprar bienes o servicios con su tarjeta de crédito o pedir préstamos.

En este sentido, las plataformas virtuales más reportadas por los usuarios son, WhatsApp, mensajes de texto, correos electrónicos, sitios web no reconocidos, además, algunos consiguen

ser perfiles públicos, en redes sociales u otros servicios online, así es como se configura este fraude electrónico causado por ciberdelincuentes, debido al gran avance de la tecnología y la carente seguridad de las entidades virtuales. Lo mencionado es un problema palpable en el país, el cual, no solo supone la desprotección de este grupo vulnerable, sino también, un posible incumplimiento por parte del Estado peruano de las normas internacionales, en cuanto es regla general procurar la vigilancia y defensa de los derechos de usuarios.

Así, se advierte que la exhibición de información privada no se restringe únicamente a redes sociales, señala también Google Docs o Dropbox los cuales no son sitios web seguros para recolectar datos íntimos como caracteres o documentaciones. Por ello, en caso de utilizar estas páginas para guardar información secreta, debe ser archivada y cifrada a fin de evitar detrimento al patrimonio de los usuarios.

Es por ello que, para desarrollar la propuesta, es necesario reconocer que, existe una afectación, la cual no ha sido tratada de manera adecuada por nuestro cuerpo legislativo, ni por entidades nacionales, menos aún por privadas, asimismo, es necesario reconocer la imposibilidad en los diversos sectores de nuestro estado. Por lo que, desde ya, las circunstancias para los clientes son frágiles y poco favorables. Desde un punto de vista crítico deducimos que, nuestro ámbito nacional no ha conseguido efectuar favorablemente mecanismos necesarios para favorecer a los usuarios.

Nuestra legislación nacional según lo establecido en el Código de Protección y Defensa del Consumidor (Ley 29571), consideran como interesados a personas naturales o jurídicas que obtienen, monopolizan o gozan como receptores finales servicios o mercancías materiales e inmateriales, en favor conveniente o de su grupo familiar o social, procediendo así en una esfera ajena a una actividad empresarial o profesional. No considera interesado para efectos de este Código a quien consigue, maneja o goza de una ganancia o prestación regularmente consignadas para los desenlaces de su prontitud como consignatario.

3.1.2 Medidas de protección jurídica frente al phishing

En este apartado, revisaremos los elementos de resguardo de las entidades públicas y privadas tras el impacto tecnológico en nuestro país, adicional a ello, el estado de emergencia nacional que se vivió durante los últimos años a consecuencia de la pandemia del Covid -19, concibiendo una transformación en la era digital. Así se advierte, que más usuarios prefieren emplear medios de pago analógicos para realizar sus operaciones; existiendo, además, un gran número de nuevos usuarios incorporados.

Desde la postura de la SBS, el marco regulatorio ejecutar técnicas de supervisión in situ y extra situ, referentes al servicio de ciberseguridad y amenazas que afrontan diversas entidades

financieras; añade evaluar su organización, políticas, asignación de recursos prácticas de gestión y herramientas preventivas de localización y respuesta. Para este efecto, durante el año 2019 se realizó un nuevo marco normativo de tarjetas de crédito y débito, para proteger a los usuarios, añadiendo obligación de los emisores e implementar reformas en los mecanismos de seguridad al efectuar transacciones.

No obstante, la Superintendencia de Banca, Seguros y AFP inspecciona y restablece habitualmente su marco regulatorio y de verificación a la seguridad de la información y ciberseguridad, instando a las entidades inspeccionadas que realicen de manera apropiada la organización interna y tecnológica demandada para formalizar la ciberseguridad.

De manera que, el Instituto Nacional de defensa de la idoneidad y del resguardo de la propiedad intelectual (en adelante INDECOPI) no es ajena a nuestra actual coyuntura como lo es el phishing y es por ello que, en su Resolución Final N° 2014-2016/CC1, instituye que; todo distribuidor brinda una garantía sobre la idoneidad de los acervos y transacciones que promete en el mercado. En tal sentido, para implantar la efectividad de una transgresión incumbirá al usuario o a la autoridad administrativa certificar la objetividad del menoscabo, siendo este 24 escenario la obligación del proveedor indicar que dicho desperfecto no le es atribuible para ser absuelto de responsabilidad.

Es vital considerar para el presente estudio la Ley de delitos informáticos, misma que refiere prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos, perpetrados mediante el uso de tecnologías de información o comunicación, con el propósito de garantizar la lucha eficaz contra la ciberdelincuencia. En consecuencia, la discapacidad de protección en nuestro sistema nacional comprende deficiencias en su actuación, limitaciones al proteger bienes patrimoniales y la inexactitud de restricciones de las entidades.

La Guía de seguridad UJA Phishing, (2018) enumera las siguientes recomendaciones que deberíamos tener; aprender a descubrir un correo de phishing, no brindar información confidencial, más aún si nos requieren caracteres, números de tarjeta de crédito, etc., ser cautelosos para rellenar formularios en páginas web, no tomar en cuenta mensajes de correspondencia electrónica de desconocidos y nunca hacer clic en los enlaces que contengan acceso a una página web.

En esta misma línea de ideas, es preciso mencionar a INDECOPI, Para defenderse frente a infracciones del phishing, los usuarios pueden tomar algunas precauciones de seguridad que pueden proteger las cuentas en caso de emergencia, es por ello, que algunas entidades han señalado posibles soluciones o tratativas dentro de cada ámbito.

En este sentido, las entidades financieras siendo las más vulnerables a diversos ataques debido a su constante exposición, incurren en una nueva batalla impulsada por la transición de la vida digital, cobrando fundamento los quebrantamientos y desacatos cibernéticos que han ajustado su enfoque a financieras, aseguradoras y más empresas que posean una poblada base de identificaciones de clientes, los cuales logren convertir en víctimas de fraude. Por lo tanto, uno de los bancos más significativo de nuestra esfera nacional, el Banco de Crédito del Perú (BCP), han reforzado medidas incluyendo gestión de riesgos de ciberseguridad.

De esta manera, es preciso mencionar la entidad privada Cineplanet, quien el pasado enero sufrió la modificación de datos de cientos de beneficiarios que albergaba la compañía en el servidor público Microsoft Azure, con las identificaciones se lograrían proveer a los cibercriminales una cadena de ataques estas modalidades son comunes, por lo cual se insta a la población a ser cuidadosos al ingresar sus datos personales.

Es importante señalar que, según Trejo (2019) carecemos de dispositivos apropiados informativos que producen grandes contingencias en la relación existente entre cliente y banco, es por ello que, incidimos en la afectación de la banca electrónica cuyos parámetros de seguridad instaurados por cada sitio no brindan la confidencialidad necesaria que se ajusta a la actualidad, sobre todo por las diversas modalidades de ciberdelitos.

3.2. El phishing en el sistema financiero y sus implicancias jurídicas

En nuestro país, cada año son cientos los usuarios que reportan afectación sobre su patrimonio, sin embargo, aún no existe un tratamiento eficaz y efectivo de los bancos hacia una protección del mismo para evitar la vulneración de los derechos. Entonces, debemos observar con detalle que, la no implicancia jurídica del phishing, a pesar de, su continua afectación a organizaciones e individuos sigue causando desasosiego sobre sus datos compartidos en redes sociales.

• Impacto económico

Para Rueda (2020) la seguridad en el uso de los medios digitales es compone significativo en la coyuntura para el beneficio monetario de un estado. Así que algunos países han incorporado diferentes estrategias, políticas y normatividad para la ciberseguridad y ciberdefensa adicionalmente, han orientado a fortificar las instituciones del gobierno, apoyar al sector privado y al usuario del común. Sin embargo, la evolución de los ataques informáticos llega más allá de los esfuerzos realizados y han impactado de forma negativa esta confianza digital en los usuarios y organizaciones del país. (pág. 62)

El Instituto Peruano de Economía ha señalado que las instituciones formadas en el sistema financiero obtienen regulación del capital hacia la deuda o inversiones, existiendo ineludible

representación de terciarios financieros como los bancos, mediante el uso de instrumentos financieros, es preciso mencionar que, el sistema financiero es determinado como el conjunto de corporaciones tanto como mercados, que admiten regularizar los ahorros divisados hacia dispositivos que requieren fondeo para resguardar su déficit.

• Impacto social

Es así como, el sistema financiero compone una pieza fundamental en nuestra sociedad, mediante el avance de prontitudes financieras como la transmisión de caudales, es viable el uso de capital de manera más segura y se obtiene mayor renta, se debe agregar también que constituye una herramienta transcendental para controlar ciclos económicos permitiendo acoger políticas o medidas necesarias para estabilizar el caudal.

En la Revista digital de Ciencia, Tecnología e Innovación, se equipararon que las redes sociales más utilizadas son; Facebook, Twitter, Instagram, YouTube y LinkedIn, las cuales se generan ataques y vulnerabilidad de información personal por falta de conocimiento sobre los mismos, por lo tanto, se considera un tema actual, complejo y pertinente debido al quebrantamiento de posibles ataques y amenazas, cabe recordar que al ser redes muy activas permiten su manejo desde cualquier dispositivo tecnológico y su incorrecta gestión tiene un gran impacto en nuestra información personal. (Martínez Chérrez y Ávila Pesantez, 2020)

En consecuencia, como ya hemos venido explicando, el sistema financiero peruano requiriere atención particular y un enfoque estructurado que permita asegurar la información de manera proactiva necesitando un sistema de seguridad y gestión oportuno, asimismo medidas que imposibiliten la actuación de sistematizaciones no acreditadas sobre un sistema o red informática, dado que, existen derechos fundamentales que deben ser resguardados.

3.2.1. Implementación de la ciberseguridad en el Perú

En nuestro ámbito nacional, recientemente, ha incorporado el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, a través de la Resolución SBS N° 504-2021, desarrolla originalmente aspectos sobre seguridad de la información en un contenido de "ciberespacio". Esta normativa implanta prácticas imperceptibles en el factor de ciberseguridad y uso de interfaces de codificación de aplicaciones, generando un conjunto de protocolos que permiten la interacción entre software, para la provisión de servicios en línea. (Vodanovic, 2021)

Por ello, para vislumbrar los peligros por industria tecnológica, es preciso mencionar que el Estado peruano, se encuentra suscrito dentro de la innovación tecnológica para suministrar servicios (TIC), entre las principales actividades están el agua y electricidad, estos cuentan con

un software para su gestión y monitoreo, es decir, si vulneran estos programas por un malware o virus informático se afectarían su funcionamiento.

En la coyuntura actual los sistemas informativos de entidades estatales son atacados por hackers, puesto que no contamos estándares de eficacia apropiados por la Oficina Nacional de Gobierno Electrónico e Informática debido a su excesivo valor comercial, no han sido implementados con las normas ISO 17799 y 2700. Nuestro país en la esfera Latinoamérica es uno de los países con escasa conciencia en términos de regular la protección y riesgos en seguridad informática, siendo, uno de los países con desprovisto de legislación sobre ciberdefensa y ciberseguridad.

Esta nueva forma de vida cibernética ha traído consigo innumerables beneficios y facilidades en nuestro día a día, sin embargo, la tecnología también necesita utilizarse de manera correcta para proteger nuestra información de criminales cibernéticos. En efecto, las normas ISO son pautas metodologías que certifican la calidad, seguridad y eficacia de datos, a continuación, se indicarán algunas normas que deben adherirse a nuestro sistema financiero:

• Norma ISO 27001: Sistema de gestión de la seguridad

Es una regla que examina diversas programaciones y esquemas para ejecutar el proceso de protección de la información basada en planificar, hacer, controlar y actuar, fundamentales en la cimentación del sistema de seguridad, aquellas admitirán organizar, controlar y mitigar peligros sobre su importante activo, es decir, la información. Ahora bien, para dicha actuación se necesitará; examinar y valorar riesgos, efectuar controles, establecer un tratamiento de riesgos o esquema de mejoras, comunicar a las partes sobre los objetivos para realizar los procesos, finalmente realizar auditorías internas y externas dentro de las plataformas virtuales para evaluar la efectividad.

• Norma ISO 12812: Banca básica

El ingreso financiero en sitios web y aplicaciones móviles (app) permiten millones de transacciones diarias a usuarios y empresas para realizar pagos, contratar servicios, etc.; mediante su perfeccionamiento de la tecnología se proveerá un catalizador para purificar u optimizar la experiencia del consumidor y preservar su bienestar.

• Norma ISO 31000: 2018 Gestión de Riesgos

Esta norma examina los medios socio-económico de las empresas y las relaciones existentes, de esta manera equipara las dificultades e insuficiencias, además del impacto en la planificación cualquier tipo de organización en las entidades financieras.

3.2.1.1 Establecer medidas bancarias de responsabilidad administrativa ante el phishing.

La responsabilidad que debe otorgarse a los bancos frente al fraude informático phishing, corresponde ser aplicada de forma radical y sancionadora, buscando que los bancos asuman responsabilidad por muchas veces se pretende exigir el uso de plataformas digitales, existiendo usuarios que desconocen su manejo, cayendo en casos de error y lo más caótico ser víctimas en delitos cibernéticos.

Aunado a ello, es preciso mencionar que el banco tiene una responsabilidad directa, ya que entes que esgrimen plataformas digitales, concurren al presente usuarios que prefieren acercarse a una entidad bancaria, sin embargo, debido a la pandemia se añadieron nuevas operaciones que únicamente son efectuadas por la banca de internet, desamparando a los usuarios frente a eventuales fraudes, introduciendo circunstancias de desprotección.

Al respecto, las entidades financieras corresponden asumir una responsabilidad civil objetiva, además, el banco debe compensar el daño al patrimonio del usuario quien confió en el ente encargado, pero no se otorgó las medidas correspondientes ante esta nueva modalidad de robo de información financiera y debido a situaciones repetitivas generadas durante los últimos años corresponde otorgar medidas para contrarrestar, ya que, la entidad conoce la peculiaridad de actuación del phishing.

Por otro lado, recomendamos a los bancos o entidades financieras que ofrecen un servicio y obtienen beneficio implementar medidas adecuadas y ofrecer alternativas competentes, a fin de procurar velar por los derechos del cliente ante las diversas modalidades de estafas, de manera contraria, la entidad debe responsabilizarse de forma objetiva. Asimismo, señalar el daño generado por culpa del banco y en consecuencia, la responsabilidad total por ofrecer servicios y no poseer la seguridad apropiada a fin de impedir daños y perjuicios en el patrimonio del usuario.

3.2.1.2. Criterios de Indecopi respecto de Phishing: INDECOPI - Nº 239-2019/PS0-INDECOPI-JUN

En el marco jurídico a la ley general de protección del consumidor, el Instituto Nacional de Competencia y Protección Intelectual (INDECOPI), está autorizado para instar el respeto de normar referentes de competencia, la amparo al consumidor y derechos de propiedad intelectual, en diversos sectores, incluidos los servicios financieros, dichas facultades contienen la autoridad de ejecutar indagaciones, acoger medidas correctivas y atribuir sanciones.

Mediante la Resolución Final N°0601-2016/CC1, se denunció al Banco de la Nación (en adelante Banco) por una presunta infracción y desprotección de derechos; debido que, el señor Juan Carlos Castro Malarin miembro de las Fuerzas Armadas del Perú (en adelante FAP) señala la apertura de una cuenta de ahorros en el Banco, reconociendo su última operación el 25 de

febrero de 2014, con un saldo de S/22,66, posterior a ello, el día 24 de noviembre del mismo año se inició el fraude a través de internet con el pago de "cupones factura" por el monto de s/22,00, sin embargo, desconocía esta operación.

Asimismo, el 30 de enero del 2015 la FAP depositó a su cuenta el importe de s/23 562,60 del cual tampoco tuvo conocimiento, el 31 de enero, 1 y 2 de febrero del año en mención se efectuaron transferencias desde su cuenta a terceros del mismo Banco por s/ 1 500, durante tres oportunidades, tiempo después el señor Castro solicitó que la devolución al Banco por los importes transferidos, además de la ejecución de aparatos de seguridad que imposibiliten la verificación de los hechos similares a futuros clientes.

Ahora bien, el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor declaró infundada la denuncia interpuesta por el señor Castro contra el Banco argumentando que, al ingresar a la plataforma de internet – multired virtual, se requería el ingreso del número de la Tarjeta de Débito Multired Global, el código CVV" y la clave personal de cuatro dígitos, luego, el usuario debe contar con el sello de seguridad, clave de internet de seis dígitos y tarjeta de coordenadas, todo ello para efectuar cualquier operación por internet.

Por lo expuesto, es preciso mencionar el deber de idoneidad, la Constitución Política del Perú marca que el Estado resguarda a los clientes y beneficiarios, por lo tanto, atribuye deberes que el proveedor corresponde cumplir en la comercialización de productos o asistencia de servicios en el mercado, mediante un trato equitativo y justo a la protección que involucren desinformación o información equivocada a los consumidores.

Para finalizar, debemos solicitar una garantía tácita respecto de la idoneidad de los bienes y servicios que promete el mercado financiero, en función de la información transferida expresa o tácita, acreditando la infracción administrativa del consumidor o el ente administrativo, incluyendo existencia del defecto y el proveedor buscará probar que el menoscabo no es atribuible para ser absuelto de responsabilidad.

3.2.1.3. Análisis de Jurisprudencia: Casación 956-2017 Lambayeque

Entre los casos más emblemáticos y conocidos referentes al phishing que explica de manera detalla y la operación que se realiza es el Caso "Empresa Transporte Chiclayo Sociedad Anónima (en adelante Empresa de Transportes) contra el Banco Continental Sucursal Chiclayo" (en adelante Banco). La Sala Civil Transitoria de la Corte Suprema de Justicia de la República, efectúa un análisis sobre la afectación del patrimonio de los usuarios, además, se analiza la responsabilidad que debe o no adquirir la entidad bancaria.

En este caso, el debate radica entre la Empresa de Transportes quien demanda por daños y perjuicios al Banco, manifestando haber sufrido desfalco en sus cuentas bancarias ocasionado

por un servicio vía internet, proporcionado por la entidad financiera en virtud de los contratos celebrados. En junio de 2003, la Empresa de Transporte y la Entidad Bancaria firmaron el primer contrato de Continet Empresas, luego, suscribieron un segundo contrato de Continet en el mes de diciembre del 2006, siendo que por dicho servicio se paga una contraprestación.

Mediante ambos contratos se establecieron entre sus cláusulas la siguiente, el Banco no concedería operaciones solicitadas a través del Sistema Continet Empresas a usuarios desconocidos que no tengan facultades reconocidas o que excedan cualquier forma o monto, asimismo, acordaron que el cliente asumiría la responsabilidad de todas las operaciones realizadas mediante el Sistema Continet.

En ese contexto, el supremo tribunal reflexiona los fallos de las instancias enuncian las razones fácticas y jurídicas que respaldan y determinan la petición de indemnización por daños y perjuicios, en este caso, es infundada. Por consiguiente, concluye que tales decisiones están correctamente motivadas y aquella no afectan el debido proceso.

En este caso, la propia Empresa presentó las recomendaciones de seguridad ante fraude por Internet, no obstaculizando que le fueron entregadas a tiempo, pues lo que fundamenta en su petición es que el Banco al momento de ejecutar los movimientos no autorizados correspondió informar como atañe en diferentes cuestiones.

Aunque la empresa alegaba que el Banco incurrió en culpa inexcusable esto no se reflejó en los fundamentos ni pruebas de su demanda, pues no manifestó ni demostró con medios de prueba idóneos que el Banco haya incumplido con el contrato, es por ello juzgador concluye que el Banco sí cumplió con sus obligaciones.

Debemos tener en cuenta que, un mal manejo de claves y sistema de seguridad por parte de Clientes que no son cuidadosos, puede traer la generación de delitos informáticos. Sin embargo, asumir que en estos casos los bancos deben indemnizar a su cliente sólo porque su “actividad genera mayor utilidades” traería como consecuencia pérdidas para el sistema financiero y el desincentivo de los clientes por observar las medidas de seguridad para proteger su dinero.

Entonces, teniendo en claro los puntos mencionados en los párrafos anteriores el artículo 1319 del Código Civil, señala que la culpa inexcusable es ejercida por negligencia grave no ejecuta obligación, añade que el resarcimiento entre las empresas por la inejecución del deber parcial, tardío o defectuoso.

3.3. Medidas proactivas del sistema financiero frente al phishing

En esta misma línea de investigación con lo desarrollado en este proyecto, el phishing busca que la víctima reciba un correo electrónico que suplanta la identidad de una empresa y que se

informa de algún tipo de error o problema con los datos otorgados a través de solicitudes o por los datos bancarios del usuario.

Para prevenir este tipo de fraudes, se mencionarán algunas medidas que se pueden emplear para que el usuario receptor de estos correos de estaba debe corroborar que el emisor –entidad bancaria- del correo electrónico pueda conocer si se encuentra ante un caso de phishing, se puede discernir de manera sencilla, cuando el contenido del mensaje no corresponde con la situación de una persona, por ejemplo, podremos sospechar cuando nos remita un correo indicando que hemos adquirido un premio económico. (López, 2019)

Como ya lo hemos adelantado en las primeras páginas de esta investigación, nuestro objetivo es contribuir razonamientos legales aplicables en la regulación del phishing para prevenir vulneraciones a los usuarios. Por lo tanto, se plantearán pautas que ofrezcan como base y directriz en los diversos procesos de atención a las innumerables solicitudes de los beneficiarios para proteger su patrimonio.

Hemos querido introducir, de manera específica algunas medidas para que el sistema financiero funcione en circunstancia ópticas, reduciendo consigo los consumos fraudulentos generados por el phishing, las cuales giran en torno a las siguientes ideas:

• Educación a los consumidores

Es oportuno mencionar que, existe un reciente desarrollo e implementación de campañas de información y alertas dirigidas a los ciudadanos a fin de evitar riesgos, sin embargo, estás no son suficientes, pues deben amplificar con vídeos informativos, flyer al ingresar las aplicaciones o páginas web, incluso el personal de las entidades deben advertir sobre las modalidades de ciberdelincuencia existentes, a fin que los beneficiarios adopten buenas prácticas que contribuyan de manera eficaz y masiva.

• Generar códigos y/o palabra o pregunta secreta

Otra alternativa idónea es, la codificación directa de las entidades bancarias, utilizando número, letras o ambas, asimismo, al realizar algún movimiento mediante el aplicativo o sitio web, se debe añadir la opción de escribir una pregunta secreta, por ejemplo: ¿la ciudad en la que naciste?, preferencias, etc.

• Notificar y denegar el acceso tus cuentas bancarias al desconocer el dispositivo no vinculado

Existe una actuación previa al adquirir o inaugurar una cuenta bancaria, siendo esta el registro de información confidencial, entre los ítems a completar se encuentra el número del móvil que desea vincular, por tanto, si se reconoce un nuevo ingreso desde un dispositivo no

reconocido y/o incógnito, una medida idónea será advertir dicha actuación al beneficiario y de manera inmediata notificar y denegar el acceso.

• Seguros contra fraudes cibernéticos

Establecer seguros para casos de consumo fraudulentos, en ellos el cliente tendrá acceso a elegir diversas compañías de seguros y el alcance de la cobertura para operaciones como; transferencias bancarias, pago de servicios y/o entidades, retiros, giros, entre otros no reconocidos por el usuario.

Ahora bien, todos los mecanismos señalados líneas antes se puede atender desde un dispositivo móvil, pero también es importante mencionar que existe gran parte de la población nacional carente de Smartphone o celulares inteligentes y menos aún de su manejo, ello es indicador clave para cierto grupo especial, reflejando así un estado doble de vulnerabilidad, para ellos nuestro país no ha tomado acuerdos referentes a sus necesidades, por ende, buscaré proponer alternativas de solución digitales:

• Enseñar el DNI ante la pantalla

Al ingresar a la página correcta a través de laptop o pc, se solicitará mostrar el DNI mediante la cámara del dispositivo tecnológico y digitarlo. Después de haber repasado los diversos mecanismos de protección, corresponde señalar su aplicación bajo el principio de idoneidad, cuyo objetivo es proteger el derecho constitucional del usuario frente al phishing competente al sistema financiero, lo cual no se demuestra en la experiencia, puesto que, existe una carente protección como se ha evidenciado a lo largo de este análisis, por ello, se sugiere su implementación.

Otro de los mecanismos de prevención de fraudes en un sistema de información, es a través de la identificación de cuentas individuales y mancomunadas del personal que trabaja en la entidad bancaria, detectando hackers para conocer si se realiza la operación financiero segura, o si este movimiento bancario es adecuado a nuestras operaciones habituales, además, deberá verificar la actuación le corresponde al usuario, de lo contrario, procesa de manera inmediata a bloquear la ejecución de dicha actuación.

Finalmente, para concluir este ítem, es preciso describir una postura a favor del tema puesto que, mediante la implementación de sistemas de información se proyecta subyugar el catálogo de reclamos por fraude y de manera contraria generar un bienestar directo en los consumidores, además, mejorar el prestigio de la entidad financiera ofreciendo seguridad a sus usuarios promoviendo el desarrollo de una bancarización segura y confiable.

Conclusiones

Las principales implicancias existentes en el sistema financiero por fraudes ocasionan pérdidas económicas debido a ineficaces sistemas informáticos relacionados por el bajo control interno de las entidades bancarias y por la carente seguridad en las plataformas informáticas, asimismo, el impacto social al suplantar la identidad de los usuarios, su tratativa es efímera y poco adecuada frente a los peligros en la web.

Nuestra legislación nacional deberá generar pautas de información esencial y apropiadas que permitan advertir y reducir la cantidad de fraudes, añadiendo estrategias de navegación tangibles para los usuarios, accediendo a seguros de tarjetas, implementación de estrategias informáticas mediante el uso de ISO, a fin de reconocer cuando son víctimas de ataques de phishing basados en políticas de seguridad de la organización bancaria permitiendo a los usuarios verificar de manera automática el sitio web al que se encuentran conectados.

Recomendaciones

Se recomienda al Sistema Financiero Peruano y la Superintendencia de Banco y Seguro que el phishing al ser un fraude electrónico con carente tratativa y nuevo en nuestra legislación, el Estado Peruano deberá velar e incorporar una normativa adecuada que permitirá salvaguardar los derechos de los consumidores, es por ello, que mediante este trabajo, se insta a las entidades encargadas a regular medidas coercitivas adecuadas que faculten a los consumidores a su protección en la actualidad y prever futuras problemáticas.

Referencias

1. Aguirre Quezada, J. P. (2022). Ciberseguridad, desafío para México y trabajo legislativo. (Vol. Cuaderno de investigación No. 87). México: Instituto Belisario Domínguez Senado de la República. http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5551/Cuaderno%20de% 20Investigaci%C3%B3n%2087.pdf?sequence=1&isAllowed=y
2. Ananías Navarro, F. (2020). Análisis comparativos del Phishing y de responsabilidad civil de los bancos previa y posterio entrega en vigencia de la Ley 21.234. https://repositorio.udd.cl/bitstream/handle/11447/4112/An%C3%A1lisis%20comparativo%20del%20phishing%20y%20responsabilidad%20civil%20de%20los%20bancos.pdf?sequence=1 &isAllowed=y
3. Aroni Córdova, N., & y Barrios Elías, R. (2018). Análisis de los principales factores financieros y de la reputación empresarial que vienen siendo impactados por el incremento de los delitos informáticos en los principales bancos del Perú. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625668/Aroni_cn.pdf ?se quence=1&isAllowed=y
4. Asobancaria. (2019). Saber más, ser más. Programa de educación financiera de los bancos en Colombia. https://www.sabermassermas.com/phishing/
5. Apaza Chavez, W. A. (2021). Propuesta de un plan de seguridad de la información para incrementar la fiabilidad de datos en una financiera. 2. doi:2708-0935
6. Barrantes Centurion, J., Sánchez Silva , J., & Gutiérrez Garcia , S. (2020). Seguridad de la información: ¿Cómo proteger los datos personales? https://boletin.ins.gob.pe/wp-content/uploads/2020/2020a%C3%B1o26(3- 4)/a06v26n3_4_2020.pdf
7. Benavides, E., Fuertes , W., & Sanchez , S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. https://revistas.uteq.edu.ec/index.php/cyt/article/view/357/407
8. Castillo Rubiano, Ó. (2021). Phishing: Día de pesca. Bogotá, Colombia. https://bdigital.uexternado.edu.co/server/api/core/bitstreams/e8eac144-41c1-4efea7a8-85d8f4f93097/content
9. Cisco Cybersecurity series. (Junio de 2019). Correo electrónico: pulse con precaución. Cómo protegerse contra el phishing,el fraude y otras estafas. https://www.cisco.com/c/dam/global/it_it/products/security/pdfs/cybersecurityseries_email_es_def.pdf

10. Código de protección y defensa del consumidor. LEY Nº 29571.- Código de protección y defensa del consumidor. https://www.gacetajuridica.com.pe/boletinnvnet/img_bol08/Codigo%20de%20proteccion%20y%20defensa%20del%20consumi dor.pdf
11. Constitución Política del Perú. (1993).
12. Defensor del cliente financiero. (2008). Boletín del denfensor del cliente financiero. Lima.
13. Flores Cáceres, C. (Enero de 2017). El phishing como comportamiento penalmente relevante. http://opac.pucv.cl/pucv_txt/txt-4000/UCC4478_01.pdf
14. Guerrero Lozano, B., & Castillo Caicedo, D. (2018). Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano. https://repository.unad.edu.co/bitstream/handle/10596/13387/52498805.pdf?sequence=5&isAllowed=y
15. Giraldo Martinez, J. P., & Duarte Pacheco, I. G. (23 de noviembre de 2018). Ingeneria social: técnica de ataque de phishing y su impacto en las empresas colombianas. Ingeneria social: técnica de ataque de phishing y su impacto en las empresas colombianas.: https://repository.unad.edu.co/bitstream/handle/10596/27050/jpgiraldoma.pdf?sequence=1&isAllowed=y
16. Hancco Zapana, E. (2017). “La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú - 2017”. http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y
17. Hérnandez Mejia , D., & Mendoza Flores , G. (2018). El funcionamiento del comercio electrónico, categorías seguridad para usuarios demografia de usos habituales. http://ri.uaemex.mx/bitstream/handle/20.500.11799/95210/TESIS-COMERCIOELECTRONICO.-Definitivo...pdf
18. Huerta , I. (2021). Phishing:métodos de estafa en comercio electrónico en México. Transdigital, 10.
19. Kenet Venancio, A. (Mayo de 2021). Evolución de la investigación criminal en el robo de información personal (phishing), acoso pederasta (grooming) y suplantación de identidad (spoofing). http://recursosbiblio.url.edu.gt/tesiseortiz/2021/07/03/YacKenet.pdf

20. López Sanchez, J. (enero de 2019). Métodos y técnica de detección temprana de casos de phishing. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89225/6/jlopezsanchez012TFM0119memoria.pdf
21. Mariano Díaz, R. (2020). La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad. FAL Boletín 382, 3. https://repositorio.cepal.org/bitstream/handle/11362/46275/1/S2000679_es.pdf 36
22. Martínez Chérrez, W. E., & Ávila Pesantez, D. F. (2020). Ciberseguridad en las redes sociales: una revisión teórica. Revista digital de Ciencia, Tecnología e Innovación
23. Medina Martínez , J., Cárdenas Osorio , C., & Mejia Lobo, M. (2021). Análisis del Phishingy la Ley de delitos informáticos en Colombia. https://revia.areandina.edu.co/index.php/vbn/article/view/1948/1870
24. Mengoa Valdivia , M. (2021). Punibilidad del comportamiento del phisher- muler en el delito de fraude informático en el Perú. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62379/Mengoa_VMMSD.pdf?sequence=1
25. Organización de los Estados Americanos. (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf
26. Organización de los Estados Americanos. (2019). Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. (1era edición ed.). Colombia. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sectorfinanciero-para-Colombia-y-America-Latina.pdf
27. Ormachea Montes, J. (2019). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. https://renati.sunedu.gob.pe/bitstream/sunedu/1336266/1/TESIS%20para%20optar%20Grado%20de%20DOCTOR_Juan%20ORMACHEA%2016_07_20.pdf
28. Paredes Pérez, J. (2013). De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y
29. Parra Perea, R. (2016). “Proyecto legal para un esquema nacional de ciber seguridad”. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/2051/parra_prg.pdf?sequence=1&isAllowed=y

30. Profeco. (2021). Revista Profeco comportamiento de tiendas virtuales. https://www.gob.mx/profeco/prensa/revisa-profeco-comportamiento-de-tiendasvirtuales?state=published
31. Rivera Davila, A. (2019). Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016. http://repositorio.undac.edu.pe/bitstream/undac/1372/1/T026_04066691_M.pdf
32. Rosero Tejada, L. (2021). El phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático. https://dspace.ups.edu.ec/bitstream/123456789/21699/4/UPS-GT003573.pdf 37
33. Rueda Quintero, J. A. (2020). Estudio monográfico: Impacto de la técnica de ataque de phishing en Colombia durante los últimos cinco años. https://repository.unad.edu.co/bitstream/handle/10596/38721/jaruedaq.pdf?sequence=1&isAllowed=y
34. Santos Sanchez, B. I. (2021). Aspectos técnicos del delito de phishing. https://buleria.unileon.es/bitstream/handle/10612/13693/SANTOS%20S%C3%81NCHEZ%2C%20BLANCA%20IRIS.pdf?sequence=1&isAllowed=y
35. Schwalb, M. (2020). Quincuagésima reunión Intercampus. Reflexiones a propósito del Código de Protección y Defensa del Consumidor. Lima.
36. Superintendencia de banca y seguros. (mayo de 2018). SBS Informa Boletín Semanal. https://www.sbs.gob.pe/Portals/0/jer/BOLETINSEMANAL/2018/BoletinSem17_2018.pdf
37. Superintendencia de Banca, Seguros y AFP. (2021). Ciberseguridad: construyendo resiliencia en el sistema financiero. https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1213
38. Superintendencia de Banca, seguros y AFP. (2019). Regulación del sistema financiero peruano consistente con los mejores estándares interncionales de regulación prudencial. https://www.sbs.gob.pe/Portals/0/Archivos/2019_01.%20Implementaci%C3%B3n%20de%20Basilea%20en%20el%20Per%C3%BA.pdf
39. Universidad de Jaén. (2018). Guía de seguridad UJA Phishing. https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%202.%20Phishing.pdf
40. Vodanovic, L. (2021). Panorama regulatorio. Fintech Latam 2021-2022. Vodanovic Legal, 13. https://vodanovic.pe/wpcontent/uploads/2021/12/REPORTE_FINTECH_2021.pdf

41. Zabala, A. (2020). Responsabilidad bancaria frente al delito de phishing en Colombia. https://repository.ucatolica.edu.co/bitstream/10983/14943/1/Art%C3%ADculo%20Phishing%20-%20Alexander%20Zabala.pdf