FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

EL DELITO DE PHISHING EN LAS ENTIDADES FINANCIERAS DEL PERÚ

Trabajo de investigación para obtener el grado académico de Bachiller en Derecho

Autoras

DIAZ PARI, Angie Cecilia Cristina (ORCID**:** 000-0003-2351-0479)

GOITIA CARDENAS, Susan Emperatriz (ORCID: 0000-0002-5139-9184)

Asesora

MEDINA LOPEZ, Maria Elena (ORCID:0009-0004-5097-0491)

Línea de investigación de programa

Enfoque interdisciplinario de la ciencia jurídica

Línea de acción RSU

Desarrollo e innovación social

LIMA, PERÚ, SETIEMBRE DE 2024

Referencia bibliográfica

Diaz Pari, A. C. C., & Goitia Cardenas, S. E. (2024). *El delito de phishing en las entidades financieras del Perú* [Trabajo de investigación, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú.

HOJA DE METADATOS

Datos del autor	
Nombres y apellidos	Angie Cecilia Cristina Diaz Pari
Tipo de documento de identidad	DNI
Número de documento de identidad	71605373
URL de ORCID	https://orcid.org/0000-0003-2351-0479
Datos del autor	
Nombres y apellidos	Susan Emperatriz Goitia Cardenas
Tipo de documento de identidad	DNI
Número de documento de identidad	70854826
URL de ORCID	https://orcid.org/0000-0002-5139-9184
Datos del asesor	
Nombres y apellidos	Maria Elena Medina Lopez
Tipo de documento de identidad	DNI
Número de documento de identidad	43498466
URL de ORCID	https://orcid.org/0009-0004-5097-0491
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Martin Vicente Tovar Cerquen
Tipo de documento	DNI
Número de documento de identidad	09700062
Secretario del jurado	
Nombres y apellidos	Yda Rosa Cabrera Cueto
Tipo de documento	DNI
Número de documento de identidad	06076309
Vocal del jurado	
Nombres y apellidos	Alfonso Alvarado Vigo
Tipo de documento	DNI
Número de documento de identidad	45603621
Datos de la investigación	
Título de la investigación	El delito de phishing en las entidades financieras del Perú

Línea de investigación Institucional	Persona, sociedad, empresa y estado
Línea de investigación del Programa	Enfoque interdisciplinario de la ciencia jurídica
Línea de acción RSU	Salud y bienestar
URL de disciplinas OCDE	https://purl.org/pe-repo/ocde/ford#5.09.01

FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACIÓN DEL TRABAJO DE INVESTIGACIÓN

En la ciudad de Lima, el jurado de sustentación del trabajo de investigación conformado por: el MAG. MARTIN VICENTE TOVAR CERQUEN como presidente, la DRA. YDA ROSA CABRERA CUETO como secretario y el MAG. ALFONSO ALVARADO VIGO como vocal, reunidos en acto público para dictaminar el trabajo de investigación titulado:

EL DELITO DE PHISHING EN LAS ENTIDADES FINANCIERAS DEL PERÚ

Presentado por la egresada:

ANGIE CECILIA CRISTINA DIAZ PARI

Para que obtenga el **Grado académico de bachiller en derecho**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado – Muy Bueno** con una calificación de **DIECIOCHO (18).**

En fe de lo cual firman los miembros del jurado, el 24 de setiembre de 2024.

PRESIDENTE	**SECRETARIO**	**VOCAL**
MAG. MARTIN VICENTE TOVAR CERQUEN	DRA. YDA ROSA CABRERA CUETO	MAG. ALFONSO ALVARADO VIGO

FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACIÓN DEL TRABAJO DE INVESTIGACIÓN

En la ciudad de Lima, el jurado de sustentación del trabajo de investigación conformado por: el MAG. MARTIN VICENTE TOVAR CERQUEN como presidente, la DRA. YDA ROSA CABRERA CUETO como secretario y el MAG. ALFONSO ALVARADO VIGO como vocal, reunidos en acto público para dictaminar el trabajo de investigación titulado:

EL DELITO DE PHISHING EN LAS ENTIDADES FINANCIERAS DEL PERÚ

Presentado por la egresada:

SUSAN EMPERATRIZ GOITIA CARDENAS

Para que obtenga el **Grado académico de bachiller en derecho**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado – Muy Bueno** con una calificación de **DIECIOCHO (18).**

En fe de lo cual firman los miembros del jurado, el 24 de setiembre de 2024.

PRESIDENTE	**SECRETARIO**	**VOCAL**
MAG. MARTIN VICENTE TOVAR CERQUEN	DRA. YDA ROSA CABRERA CUETO	MAG. ALFONSO ALVARADO VIGO

ACTA DE APROBACIÓN DE ORIGINALIDAD

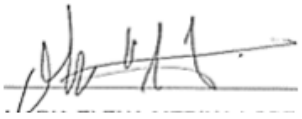
Yo Maria Elena Medina Lopez docente de la Facultad de Derecho de la Escuela Profesional de Derecho de la Universidad Autónoma del Perú, en mi condición de asesora del trabajo de investigación titulado:

EL DELITO DE PHISHING EN LAS ENTIDADES FINANCIERAS DEL PERÚ

De las egresadas Angie Cecilia Cristina Diaz Pari y Susan Emperatriz Goitia Cardenas, certifico que el trabajo de investigación tiene un índice de similitud de 10% verificable en el reporte de similitud del software Turnitin que se adjunta.

La suscrita revisó y analizó dicho reporte a lo que concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Autónoma del Perú.

Lima, 01 de octubre de 2024



Maria Elena Medina Lopez

DNI: 43498466

El delito de phishing en las entidades financieras del Perú

Phishing crime in financial entities in Peru

Angie Cecilia Cristina Díaz Pari[1], Susan Emperatriz Goitia Cardenas[2]

RESUMEN

El delito de phishing implica la clonación de sitios web para engañar a los usuarios. A nivel internacional en España en el año 2023, el 67% de las empresas privadas sufrieron un ataque de phishing. En América Latina los países más afectados fueron Brasil (134 millones de intentos de ataque), México (43 millones) y Perú (31,5 millones). A nivel nacional, en 2024 se registraron un millón de detecciones, por lo cual el objetivo del presente trabajo es demostrar la importancia de implementar el compliance en entidades financieras a fin de combatir el phishing. La metodología aplicada fue un método hipotético deductivo no experimental. La conclusión indicará al compliance como una herramienta de prevención.

Palabras clave: cumplimiento, phishing, sector financiero, seguridad jurídica

ABSTRACT

The crime of phishing involves cloning websites to deceive users. Internationally in Spain in 2023, 67% of private companies suffered a phishing attack. In Latin America, the most affected countries were Brazil (134 million attack attempts), Mexico (43 million) and Peru (31.5 million). At the national level, one million detections were recorded in 2024, which is why the objective of this work is to demonstrate the importance of implementing compliance in financial entities in order to combat phishing. The methodology applied was a non-experimental hypothetical deductive method. The conclusion will indicate compliance as a prevention tool

Keywords: compliance, phishing, financial sector, legal security

[1] Universidad Autónoma del Perú. Orcid 000-0003-2351-0479, adiaz21@autonoma.edu.pe
[2] Universidad Autónoma del Perú. Orcid 0000-0002-5139-9184, sgoitia@autonoma.edu.pe

I. Introducción

La seguridad jurídica es un principio fundamental que implica hacer prevaler el desarrollo correcto del derecho (Vargas, 2022). En el sistema financiero tiene como finalidad garantizar el desarrollo de la certeza y transparencia entre la confianza de los clientes con respecto a la protección de sus datos personales.

Sin embargo, actualmente el manejo de los datos personales por parte de las entidades financieras viene siendo vulnerado por delitos cibernéticos. Siendo uno de ellos, el delito de phishing, el cual consiste en realizar la clonación de un sitio web para engañar al usuario con el fin de que ofrezca sus datos personales como nombre, celular, DNI y hasta claves de los servicios financieros (Flores, 2020).

A nivel internacional, en España en el año 2023, el 67% de las empresas privadas sufrieron un ataque de phishing, siendo especialmente las entidades financieras. Además, las sanciones financieras como multas por incumplimientos regulatorios, aumentaron un 25% y los daños a la reputación en un 56% por la falta de conocimientos sobre ciberseguridad (Diario It Reseller, 2024).

A nivel de Latinoamérica, entre junio de 2022 a julio de 2023 aumentaron los casos del delito de phishing, pues acorde a lo expuesto por Kaspersky a través del Panorama de Amenazas para América Latina en el Diario El Comercio (2023):

> Se reportó un total de 286 millones de ataques phishing, lo que significó un incrementó en 617% en comparación con los 12 meses anteriores y un promedio de 544 ataques por minuto. Siendo los países más afectados Brasil (134 millones de intentos de ataque), México (43 millones), Perú (31,5 millones), Colombia (30,9 millones), Ecuador (12,2 millones) y Argentina (9,4 millones). Entre los cuales, los casos de phishing se dirigieron específicamente a datos financieros (42,8% - 28,40% temas bancarios, 9,40% medios de pago

y 2,70% servicios financieros).

A nivel nacional en lo que va del año 2024, se han registrado un millón de detecciones únicas de phishing en Perú, siendo la cifra más alta en los últimos años, específicamente entre los meses de mayo y junio según un estudio de la compañía de software de ciberseguridad de ESET. Asimismo, acorde al Estado del Riesgo Cibernético en Latinoamérica en Tiempos del COVID-19, del 49% de las empresas peruanas encuestadas, se percibió un incremento en los ataques cibernéticos a raíz de la pandemia, y el 21% consideró que la ingeniería social (phishing) es el ciberataque que más se ha dado (Solar, 2024).

Un claro ejemplo es lo ocurrido a inicios del presente año, en donde la ciudadana María Delgadillo sufrió un ataque de phishing que le costó la pérdida de 13 mil soles de sus ahorros en el Banco de Crédito del Perú. Siendo, que el incidente se produjo cuando Delgadillo, al hacer clic a un enlace de Facebook que la dirigía a una página web de venta de ropa, fue redirigida a un sitio web fraudulento, lo cual ocasionó que, su teléfono celular comenzará a presentar fallas técnicas y se apagará.

Posteriormente, cuando la ciudadana decide revisar su cuenta bancaria a través de la banca móvil, se percata que su saldo era de cero soles. Razón, por la cual intenta comunicarse con el Banco de Crédito del Perú, quien primeramente hace caso omiso a su queja para luego responderle mediante escrito, que era su responsabilidad por no reportarlo en su debido momento (Arce, 2024).

Ilustrándose en el presente caso la vulnerabilidad de los usuarios ante los ataques de phishing y la necesidad de que las entidades financieras brinden una respuesta más eficiente y proactiva ante este tipo de delito.

El tema tiene relevancia porque se relaciona con el impacto actual que provoca el delito de phishing en la seguridad financiera de individuos y empresas, pues en el

ámbito económico con el aumento de transacciones fraudulentas se causan considerables pérdidas financieras a las víctimas. En el ámbito social, se generan sentimientos de inseguridad y miedo a los usuarios financieros, lo cual afecta la confianza en las entidades financieras.

La importancia tanto en el ámbito académico como en la sociedad en general es establecer un análisis de los desafíos legales en relación a la protección de datos personales, la responsabilidad de las entidades financieras y la regulación de la ciberseguridad para desarrollar estrategias de prevención y mitigación de ataques de phishing.

Históricamente el tema materia de análisis ha evolucionado, siendo esta desde el año 2001, fecha en la que Estados Unidos presenta casos donde los hackers crearon sitios web falsos que imitaban plataformas de pago como PayPal. En el 2008 con la llegada del Bitcoin y otras criptomonedas se abrió nuevas posibilidades para realizar transacciones ilegales con mayor facilidad.

En el año 2018 los "kits de phishing" aparecieron en la dark web, con correos electrónicos persuasivos y enlaces que imitaban marcas reconocidas, facilitando la creación de campañas de phishing más sofisticadas.

En el año 2020, el delito de phishing consigue más notoriedad, dado que comienza con el auge de correos electrónicos fraudulentos, para posteriormente en el año 2022, incorporarse con la inteligencia artificial (IA) (González, 2024).

En tanto, en el Perú desde el año 2013 se crea la Ley Nº 30096, “Ley de Delitos Informáticos” a fin de garantizar la lucha eficaz contra la ciberdelincuencia. Sin embargo, dicha ley al año siguiente sufre una modificación por la Ley Nº 30171, donde al delito de phishing se le considera como parte del fraude informático (Aredo, 2023).

Posteriormente, mediante la resolución N.° 206-2019 se reconoce por primera

vez al delito de phishing como un tipo penal pasible de sanción a partir del caso Banco Interbank, donde se emuló la técnica conocida como “Phishing bancario” (Corte Suprema, 2020).

Por ello destacamos su pertinencia en el contexto actual, dado que a partir de lo ocurrido en la pandemia COVID.19 (año 2020) aumentaron los casos del delito de phishing, por lo que dicho tipo penal fue catalogado como una nueva modalidad de delito cibernético cometido por trabajadores de una entidad financiera.

En ese contexto se identifican las áreas de debate o controversia en la literatura existente sobre si el uso del compliance en entidades financieras es efectivo frente al delito de phishing.

Mayo (2023) señala en su tesis de magíster titulada “Análisis de técnicas de prevención, detección y ataques de phishing”, que la prevención de dichos ataques de phishing, podría darse mediante la implementación de una capa de seguridad cuando los usuarios inician sesión en algún sitio web, lo que hace que el usuario tenga que confirmar su identidad antes de tener acceso al inicio de sesión de dicha web. En ese sentido, el compliance podría ser efectivo frente a los delitos de phishing, sin embargo, dependería su implementación de cada entidad financiera.

En tanto, Toso (2021) en su artículo de revista titulado “El oficial de cumplimiento en el marco de un modelo integrado de compliance en las sociedades anónimas” precisa que la integración de algunos elementos claves del modelo de compliance con el uso dado por las sociedades anónimas es efectiva. Dado, que el compliance debe ser empleado frente al delito de phishing teniendo en cuenta el manejo interno de la empresa.

Por lo señalado se justifica la importancia del tema señalando su implicancia práctica mediante el cual se pretende que las entidades financieras protejan los datos

personales de los usuarios a través de una aplicación eficaz del compliance contra el delito de phishing. Asimismo, una justificación teórica, con el cual se busca aportar y reforzar conocimientos para futuras investigaciones acerca de que el compliance debe ser aplicado para el delito de phishing en entidades financieras.

Así como su relevancia para profesionales en el campo del derecho corporativo y penal e influencia en las políticas públicas. Toda vez que si bien en la Ley Nº 30096, “Ley de Delitos Informáticos” se reconoce al delito de phishing como parte del delito de fraude informático, cabe precisar que dicha configuración es amplia. Además, si bien se regula el compliance para que las empresas privadas como las entidades financieras lo implementen en resguardo de la seguridad jurídica, su aplicación no abarca para el delito de phishing. Por lo que, usando la legislación vigente, la Ley N° 30424, se podría incluir el delito de phishing, como aquel tipo penal pasible de aplicar el compliance.

II. Método

En la presente investigación se utilizó el método hipotético deductivo no experimental, comenzando desde hechos generales hasta lograr llegar a los aspectos específicos. Asimismo, se empleó la metodología cualitativa, que es considerada como un paradigma basado en generar teorías enfocadas en la fenomenología, hermenéutica y la interacción social (Ñaupas et al, 2019).

En ese contexto primero se filtró la información en las diferentes bases de datos para posteriormente revisar, escoger y recopilar las fuentes primarias materia de análisis a fin de garantizar la rigurosidad y fiabilidad del estudio.

Para este efecto se realizó la búsqueda en bases de datos como Redalyc, Scielo, La Referencia y Google académico, donde los términos de la búsqueda fueron los conectores booleanos OR como “delito de phishing OR compliance” y AND como “delito de phishing AND compliance”.

Como criterios de inclusión se aplicaron la metodología aplicada y el criterio de espacio. En cuanto a criterios de exclusión se empleó el tiempo, la falta de relación de la problemática y objetivo con el tema a investigar y la falta de información actual.

Encontrando que en los años 2019 a 2024 se publicaron alrededor de 29 340 artículos de investigación de los cuales se consignaron 30, pero estos últimos contenían trabajos duplicados, por lo que al momento del descarte se consignaron solamente 11 artículos de investigación. Siendo los principales hallazgos que el delito de phishing sucedía más en entidades financieras y que el compliance podría tener un impacto positivo en su mitigación. Las metodologías utilizadas eran más de enfoque cualitativo y las conclusiones obtenidas se centraron en resaltar la importancia de la implementación del compliance en entidades financieras.

III. Análisis e integración de la información

Los principales hallazgos obtenidos fueron la importancia del compliance en la prevención del delito de phishing en entidades financieras, destacando su eficacia en la mitigación de riesgos y en la preservación de la seguridad jurídica de los datos personales de los usuarios financieros.

Se identificaron patrones en la literatura que resaltan la necesidad de contar con un programa de cumplimiento eficiente, la designación de un encargado de prevención (officer compliance) y la supervisión constante del modelo implementado. Dado que el delito de phishing, desde la pandemia COVID-19, 2020 ha ido aumentado, pues este tipo penal cada vez aprovecha la inteligencia artificial para atentar y vulnerar la seguridad financiera.

Siendo las tendencias emergentes la importancia de la participación activa de la alta dirección en el proceso de supervisión y control del compliance frente al delito de phishing, el cual es una técnica utilizada por ciberdelincuentes para engañar a las personas y obtener información confidencial como contraseñas o datos bancarios, con el fin de cometer fraudes (Rodríguez, 2023).

Conforme a lo descrito, podemos comparar los siguientes análisis en donde se identifica que la efectividad del compliance en las políticas de las entidades financieras dependerá de su optimización constante en la evaluación de amenazas como mejoras (Herrera, et. al, 2023). Razón, por la cual el uso eficiente del compliance sería el mecanismo de prevención ideal para mitigar los riesgos de que una entidad financiera sea partícipe de la comisión del delito de phishing, motivo por el cual dicho tipo penal debería estar tipificado en la Ley N° 30424.

Aseveración, que comparte Chuco (2023) al señalar que: “El compliance frente a delitos de phishing sirven como prevención sobre todo para las entidades

financieras, a fin de protegerse contra multas, sanciones o indemnizaciones” (p.23).

Por lo cual, la gestión de riesgos, que consiste en identificar la categoría de exposición al peligro, es efectiva; más aún para entidades financieras que deben resguardar la seguridad jurídica de los datos financieros.

Además, al ser la gestión de riesgos una manera asertiva de realizar seguimientos referentes al manejo y el cumplimiento de la política empresarial, se relaciona bastante con la preservación de la reputación, que es otra respuesta positiva del uso de compliance (Chuco, 2023).

Por lo tanto, el compliance ayuda a cuidar y proteger el buen nombre de una entidad financiera e inclusive es un atributo efectivo al momento de crear y mantener la confianza con sus usuarios financieros.

De igual manera, Caffo & Chamaya (2022) indican que las facilidades dadas por el uso del compliance permiten eximir de responsabilidad penal a las entidades financieras ante la comisión del delito de phishing, ello siempre y cuando la implementación del programa de cumplimiento haya sido acorde a la política empresarial manejada por cada empresa.

Cueva (2021) también comparte dicha acepción señalando que la legislación peruana ampara el desarrollo de un gobierno corporativo empresarial a través del compliance, toda vez que ello genera beneficios de preservación del principio de legalidad, el cual minimiza daños; respeto a las personas, referente a la garantía que las entidades financieras deben tener con terceros, es decir la presunción de buena fe y garantía de no estar involucrados en actos delictuosos y protección de la justicia, aludiendo que el programa de cumplimiento facilita la configuración de un estado de derecho.

Sin embargo, existen diferencias en cuanto a la finalidad del compliance en el

delito de phishing, pues no solo ayuda a regular los hechos delictivos como el phishing dentro de las entidades financieras sino también proporciona beneficios sustanciales en una política empresarial al mitigar riesgos y predominar acciones correctivas tanto para los trabajadores de la entidad financiera como usuarios financieros que puedan estar afectados directa e indirectamente por el actuar de la empresa (Toledo, 2020)

Dado, que tal como señala Maticorena (2021): “La implementación del compliance no son absolutas ni globales, pues dependerá de la política empresarial de cada sociedad privada” (p.109); motivo por el cual primero debe realizarse la difusión del programa de compliance, es decir dar a conocer a todo el personal de la entidad financiera de manera detallada la cultura interna que se plasmará en la política empresarial referente a cómo prevenir y mitigar la comisión del delito de phishing.

Además, para que el compliance sea eficaz debe contar con elementos, los cuales para Sanclemente (2022) solo son dos, siendo el primero, el Officer Compliance, que en el Perú es una persona responsable de vigilar la implementación del sistema de prevención, el cual debería ser aplicado frente al delito de phishing para posteriormente, ser dado a través de un informe a la Superintendencia de Banca y Seguros de forma confidencial contando con una clave y un código otorgado.

El segundo es el Programa de Cumplimiento, que deberá contener normas de prevención, un mapeo de procesos riesgosos y medidas de prevención conforme los señala la Superintendencia de Bancos y Seguros (SBS), así como conductas ejercidas acorde a los principios éticos como el respeto y adecuación a las normas de probidad, confidencialidad, equidad, idoneidad, imparcialidad y veracidad.

Además, el contar con una supervisión seguida no solamente de la Superintendencia de Bancos y Seguros (SBS) sino también de la Superintendencia del Mercado y Valores (SMV), ayudaría a que la implementación del compliance sea

revisada de manera conjunta.

Dado que, la importancia y necesidad de que la alta dirección de la entidad financiera se involucre en la supervisión del funcionamiento del sistema de control, delegando esta tarea con ciertas limitaciones y manteniendo una comunicación frecuente sobre su efectivo funcionamiento, es otro criterio adicional que permitiría usar al compliance de manera eficaz (Corcoy, 2019).

No obstante, es de precisar que un programa de compliance requiere capacitación y monitoreo, siendo que en el primer caso alude a enseñar y explicar a todos los trabajadores que conforman una entidad financiera el fin de un programa de cumplimento para que, si hubiera sugerencias, estas puedan ser brindadas. Respecto a lo segundo, se debe precisar que como cualquier proyecto sin un debido seguimiento resulta ineficaz, por lo que el registro de si está siendo productivo o no el programa de cumplimento en la política empresarial de una entidad financiera ayudará a evolucionar y modificar las fallas que se estuvieran dando (Solis, 2020).

Afirmación que también comparte, Amaiquema (2023), quien detalla que para aplicar un modelo de compliance se debe tener un encargado que exclusivamente desempeñe su labor en el desarrollo del programa con la habilidad y eficacia de proponer mejoras. Asimismo, precisa que esos reportes constantes han de ser eficientes y actualizados, pues el delito de phishing, es un tipo penal que con la ayuda de la inteligencia artificial cada vez se vuelve más sofisticada para atentar contra la seguridad de los datos financieros de los usuarios.

Por ello, se resalta que la mayoría de autores se encuentran de acuerdo en la importancia del compliance en la prevención del delito de phishing en entidades financieras, así como en la necesidad de contar con un programa de cumplimiento eficiente y la designación de un encargado de prevención. Por otro lado, existen

inconsistencias en los resultados de los estudios en cuanto a la finalidad del compliance en el delito de phishing, ya que algunos estudios resaltan su papel en la regulación de hechos delictivos dentro de las entidades financieras, mientras que otros mencionan sus beneficios en una política empresarial más amplia al mitigar riesgos y tomar acciones correctivas para proteger a los trabajadores y usuarios financieros afectados.

Por esta razón, las futuras investigaciones deben abordar temas como la difusión detallada del programa de compliance en las entidades financieras, la capacitación, monitoreo continuo del personal y la importancia de la supervisión tanto de la Superintendencia de Banca y Seguros como de la Superintendencia del Mercado y Valores para garantizar la eficacia del compliance en la prevención del delito de phishing. Toda vez, que existe una necesidad de seguir explorando cómo el compliance puede adaptarse y evolucionar para enfrentar las sofisticadas amenazas de phishing respaldadas por la inteligencia artificial.

IV. Conclusiones

La implementación de un programa de compliance efectivo en las entidades financieras es crucial para combatir el delito de phishing. Este programa debe incluir políticas detalladas, un oficial de cumplimiento capacitado y un sistema de reportes eficiente.

La práctica al promover la implementación de un compliance eficiente que involucre la alta dirección y la supervisión constante, contribuye a la prevención de fraudes financieros y al fortalecimiento de la confianza con los usuarios financieros.

Las limitaciones inherentes al proceso de revisión presentan limitación en cuanto a la información sobre incidentes de phishing y las estrategias de compliance utilizadas por las entidades financieras, las cuales pueden ser confidenciales y por ende limitan la disponibilidad de datos para la investigación.

Asimismo, en cuanto a áreas de investigación futura, se necesita mayor análisis e información sobre la interacción entre el compliance y las tecnologías de seguridad, como la inteligencia artificial, para combatir el phishing.

Se recomienda una mayor investigación sobre la cooperación entre la SBS y la SMV en materia de compliance. La Ley N° 30424 solo reconoce la participación de la SMV en casos de delito, pero una colaboración con la SBS podría mejorar la comunicación y la respuesta a incidentes de phishing en el sistema financiero.

Toda vez que la revisión de literatura se basó en información general sobre el compliance frente al delito de phishing, pero se necesita un análisis más específico de las prácticas de compliance en las entidades financieras.

REFERENCIAS

Amaiquema, E. (2023). *Análisis del ataque del modelo Phishing en los sistemas informáticos y bancarios*. [Tesis de pregrado, Universidad Técnica de Babahoyo]. Repositorio de UTB. http://dspace.utb.edu.ec/handle/49000/14773

Arévalo, J. (2023, 23 de agosto). Ciberseguridad: Perú es uno de los países más afectados por el phishing en el último año. *El Comercio*. https://elcomercio.pe/tecnologia/ciberseguridad/ciberseguridad-peru-es-uno-de-los-paises-mas-afectados-por-el-phishing-en-el-ultimo-ano-noticia/

Caffo, J. & Chamaya, J. (2022). *Tratamiento Jurídico del Compliance Penal Como Marco Normativo para la Prevención de la Responsabilidad Penal en las Pequeñas Empresas.* [Tesis de pregrado, Universidad Tecnológica del Perú]. Repositorio de UTP. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/6784/J.Caffo_J.Chamaya_Tesis_Titulo_Profesional_2022.pdf?sequence=1&isAllowed=y

Chuco, V. J. (2023). *Implementación de un sistema compliance para prevenir delitos de corrupción en una organización local- Lima*. [Tesis de pregrado, Universidad Señor de Sipán]. Repositorio de USS. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10705/Victoria%20Judith%20Chuco%20Aguilar.pdf?sequence=1&isAllowed=y

Corcoy, M. (2019). Atribución de responsabilidad penal individual en la empresa - responsabilidad de los órganos de administración, asesores y oficial de cumplimiento. *Revista Peruana de Ciencias Penales, 1*(32), 59–96. https://rpcp.pe/index.php/RPCP/article/view/38

Cueva, H. (2021). *Criminal compliance como mecanismo de regulación de la responsabilidad penal de las personas jurídicas y prevención de delitos*

empresariales. [Tesis de pregrado, Universidad Señor de Sipán]. Repositorio de USS. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8364/Cueva%20Ruesta%2c%20Jack%20Humberto.pdf?sequence=1&isAllowed=y

De Lima, D., Batista, J., Leite, P. & Da Rosa, C. (2022). Relação entre valor de mercado e compliance anticorrupção. *Revista Pensamento Contemporâneo em Administração, 16*(2), 133-149. https://www.redalyc.org/journal/4417/441772079009/441772079009.pdf

Dreibigacker, A., Skarczinski, B. & Wollinger, R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland. PwC Deutschland* (52° ed.). IT-Sicherheit in Derwirtschaft. https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf

Flores, J. (2020). *Criminalidad compliance como mecanismo de solución a la criminalidad organizada, Chiclayo 2017*. [Tesis de pregrado, Universidad Señor de Sipán]. Repositorio de USP. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6921/Flores%20Arrasco%20C%c3%a9sar%20Joel.pdf?sequence=1&isAllowed=y

Flores, M. (2023, 28 de agosto). El sector financiero es el más usado en los ataques de phishing. *El Peruano*. https://www.elperuano.pe/noticia/221669-el-sector-financiero-es-el-mas-usado-en-los-ataques-de-phishing

Gastellier, S. (2021). *Vers une détection des attaques de phishing et pharming côté client*. [Tesis doctoral, Institut National des Télécommunications]. Repositorio de INT. https://theses.hal.science/tel-00699627

Gong, Q., Zhang, C., & Zhang, X. (2021). A novel deep learning approach for predicting stock market trends. *Frontiers in Computer Science, 8*(3), 563 - 600.

https://doi.org/10.3389/fcomp.2021.563060

González, P. (2024). Origen y evolución de las técnicas de phishing en el mundo. *Sello Legal Abogados*. https://sellolegal.com/blog/origen-y-evolucion-de-las-tecnicas-de-phishing-en-el-mundo/

Guardamino, B. (2023, 19 de diciembre). Estafas digitales dejan millonarias pérdidas en 2023: 6 mil casos en el país y criminales ya usan la IA para engaños. *Infobae.* https://www.infobae.com/peru/2023/12/19/estafas-digitales-dejan-millonarias-perdidas-en-2023-6-mil-casos-en-el-pais-y-criminales-ya-usan-la-ia-para-enganos/

Herrera, E., Barrera, K., & Rodríguez, I. (2023). Responsabilidad penal de las personas jurídicas en Perú: Una reevaluación del aforismo societas delinquere-nec punire potest a partir de una perspectiva anti conceptualista. *Revista Direito GV, 19*(20), 2317 - 6172. https://doi.org/10.1590/2317-6172202341

López, A. (2019). El trabajador con funciones de compliance officer en la empresa, en Europa y España. *Revista de Investigación del Departamento de Humanidades y Ciencias Sociales,* *3*(15), 1-20. https://www.redalyc.org/articulo.oa?id=581961489005

Manticorena, K. (2021). *Exoneración de responsabilidad de las personas jurídicas y el Program Compliance en el Perú*. [Tesis de maestría, Universidad Continental]. Repositorio de UC. https://repositorio.continental.edu.pe/bitstream/20.500.12394/9329/4/IV_PG_MDDP_TE_Maticorena_Livano_2021.pdf

Mayo, C. (2022). *Análisis y técnicas de prevención, detección y ataques de phishing*. [Tesis de Maestría, Universidad Nacional de Educación a Distancia España]. Repositorio de UNEDE. https://hdl.handle.net/20.500.14468/21393

Miranda, J. (2019). Compliance program como herramienta en la lucha contra la corrupción en Ecuador. *Revista de la Facultad de Jurisprudencia, 2(*4), 37-52. https://www.redalyc.org/journal/6002/600263661002/600263661002.pdf

Ñaupas, H., Mejía, E., Novoa, E. & Villagómez, A. (2019). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis* (5° ed.). Ediciones de la U. https://www.lopezgalvezasesores.com/descargas/metodologia_investigaci%C3%B3n.pdf

Ñunez, B. (2024, 29 de febrero). El 67% de las empresas españolas sufrió un ataque de phishing exitoso en 2023. *IT Reseller*. https://www.itreseller.es/seguridad/2024/02/el-67-de-las-empresas-espanolas-sufrio-un-ataque-de-phishing-exitoso-en-2023

Rodríguez, F. (2023). El delito de estafa informática.: ¿Es posible determinar la responsabilidad civil de la entidad financiera en base al artículo 120 del código penal como consecuencia del “phishing”?. *Revista de Derecho Penal y Criminología, 30*(06), 65 – 66. https://doi.org/10.5944/rdpc.JUNIO.2023.37387

Rodríguez, J. (2020). *An approach to the crime of fraud in its classic and computer modalities: From traditional fraud to new modalities such as Phishing*. [Tesis de maestría, Universidad de A Coruña]. Repositorio de UAC. https://ruc.udc.es/dspace/bitstream/handle/2183/27015/Rodr%C3%ADguezGarc%C3%ADaJos%C3%A9David_TFM_2020.pdf?sequence=2&isAllowed=y

Rosa, J.X. (2020). *Controle e regulação da criminalidade corporativa: revisitando os fundamentos de compliance*. [Tesis de pregrado, Universidad de Sao Paulo]. Repositorio de USP. https://www.teses.usp.br/teses/disponiveis/107/107131/tde-01082022140230/

publico/JuliaXRSilvaCorrigida.pdf

Sana, G. & Guarido, E. (2020). Mechanisms for risk elimination of a compliance trap in the brazilian telecommunications industry. *Revista de Administração Mackenzie, 22*(5), 1518-6776. https://www.redalyc.org/journal/1954/195468281006/195468281006.pdf

Sanclemente, J. (2022). El compliance: repercusiones en la concepción de la empresa. *Revista Escuela de Administración de Negocios, 2*(90), 193–212. https://doi.org/10.21158/01208160.n90.2021.2975

Schobel, S. (2019). *Untersuchungen zum Einfluss von Temperatur auf die Effizienz von Wärmespeichern* (6° ed.). RWTH Aachen University. https://publications.rwth-aachen.de/record/756246/files/756246.pdf

Sentencia 206-2019. (2020, 23 de enero). Corte Suprema de Justicia de la Republica del Perú (Arenas Salas, J.L.). https://img.lpderecho.pe/wp-content/uploads/2020/10/RN-206-2019-Lima-LP.pdf

Solar, D. (2024, 10 de julio). Peruanos son víctimas de ciberataques por no actualizar su sistema operativo: Más de un millón de casos de phishing en lo que va del año. *Infobae*. https://www.infobae.com/peru/2024/07/11/peruanos-son-victimas-de-ciberataques-por-no-actualizar-su-sistema-operativo-mas-de-un-millon-de-casos-de-phishing-en-lo-que-va-del-ano/

Solís, P. (2020). *Implementación del "compliance" en la micro y pequeña empresa (mype) en el Perú, importancia en la mitigación de riesgos laborales en seguridad y salud ocupacional*. [Tesis de maestría, Pontificia Universidad Católica del Perú]. Repositorio de PUCP. https://www.proquest.com/openview/fe7d2d6e2d66ca4f0198fb0e9b3f7079/1?pq-origsite=gscholar&cbl=2026366&diss=y

Suyón, K.R. (2019). *El compliance como herramienta de desarrollo para las pequeñas compañías peruanas.* [Tesis de maestría, Pontificia Universidad Católica del Perú]. Repositorio de PUCP. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/14689/SUY%c3%93N_CUADROS_EL_COMPLIANCE_COMO_HERRAMIENTA_DE_DESARROLLO_PARA_LAS_PEQUE%c3%91AS_COMPA%c3%91IAS_PERUANAS.pdf?sequence=1&isAllowed=y

Toledo, A.F. (2020). *Propuesta para las empresas en el Perú para respetar derechos humanos a través de los programas de compliance anticorrupción*. [Tesis de pregrado, Pontificia Universidad Católica del Perú]. Repositorio de PUCP. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/21

Toso, A. (2020). El oficial de cumplimiento en el marco de un modelo integrado de compliance en las sociedades anónimas. *Revista Coquimbo, 28*(3287), 0718-9753. https://www.redalyc.org/journal/3710/371070187022/371070187022.pdf

Vargas, R.A. (2022). Seguridad jurídica como fin del derecho. *Revista Scielo, 27*(2023), 2393-6193. http://www.scielo.edu.uy/pdf/rd/n27/2393-6193-rd-27-e3075.pdf