FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

El phishing y su vulneración a la protección de datos personales en los delitos informáticos

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Aredo Luján, Luciano Antonio (ORCID: 0000-0002-8551-0207)

ASESOR:

Mg. Zurita Melendrez, Magdiel (ORCID: 0000- 0002-7373-1432)

LÍNEA DE INVESTIGACIÓN

Derecho penal

TRUJILLO – PERÚ

2021

Dedicatoria

A Dios, por permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi madre, por ser el pilar más importante y por su apoyo incondicional sin importar nuestras diferencias de opinión. A mi padre, quien me apoyo en todo momento de mi vida. A mi tía, a quien quiero como a una madre, por compartir momentos significativos conmigo y por siempre estar dispuesta a ayudarme. A mi hermana, a quien estimo mucho, por apoyarme incondicionalmente y compartir un vínculo único que no se extinguirá jamás. A mi hermano Ricardo Aredo, porque siempre te recordaré y te llevaré presente en todo momento de mi vida, sé que nos cuidas al lado de Dios.

Agradecimiento

Los resultados de este proyecto están dedicados a todas aquellas personas que, de alguna forma, son factor fundamental para poder realizar nuestras metas.

Nuestros sinceros agradecimientos están dirigidos al Dr. Magdiel Zurita Melendrez, quien, con su ayuda desinteresada, nos brindó su apoyo para poder realizar este proyecto de manera eficaz.

A los profesores de UCV – Universidad César Vallejo que gracias a sus enseñanzas podremos lograr nuestros objetivos como profesionales de la carrera de Derecho.

A nuestras familias por siempre brindarnos su apoyo, tanto sentimental, como económico. Pero, principalmente nuestros agradecimientos están dirigidos hacia nuestros padres por brindarnos su apoyo incondicional.

A mis amigos y amigas y a todas las personas que me incentivaron y me motivaron para seguir adelante con los objetivos de este propósito.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La investigación realizada tiene como objetivo general: Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos, y como objetivos específicos: a) Explicar los alcances e impactos del phishing como apropiación de datos personales, b) Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad, y c) Analizar los presupuestos de los delitos informáticos en el código penal peruano. El tipo de investigación es de tipo básico, ya que se hace un análisis solo de documentos mas no se hará una aplicación. En cuanto a los resultados, se ve la necesaria modificación de la normativa, la forma en la que se ve afectada la persona acarrea en la comisión de otros delitos, también se debe realizar campañas mediáticas que generen cultura de prevención a fin de evitar la llamada ingeniería social. Con relación a las conclusiones, mediante el uso de engaño o ardid, se aprovechan de la poca pedagogía informática. Se debe emplear mecanismos de autenticación, como identificación dactilar y facial, token digital por mensaje de texto, resguardando los datos personales. Los presupuestos de los delitos informáticos emplean definiciones muy genéricas que no permite una correcta delimitación del phishing.

Palabras clave: Phishing, Código Penal, Ingeniería Social, tipificar, biometría.

Abstract

The general objective of the research carried out is: To determine if phishing violates the protection of personal data in computer crimes, and as specific objectives: a) Explain the scope and impacts of phishing as the appropriation of personal data, b) Explain the importance of precaution personal data as a guarantee of protection of the right to privacy, and c) Analyze the assumptions of computer crimes in the Peruvian criminal code. The type of investigation is basic, since only documents are analyzed but an application will not be made. Regarding the results, the necessary modification of the regulations is seen, the way in which the person is affected leads to the commission of other crimes, media campaigns that generate a culture of prevention should also be carried out in order to avoid the call social engineering. Regarding the conclusions, through the use of deception or trickery, they take advantage of the little computer pedagogy. Authentication mechanisms must be used, such as finger and facial identification, digital token by text message, protecting personal data. Cybercrime budgets use very generic definitions that do not allow a correct delimitation of phishing.

Keywords: Phishing, Penal Code, Social Engineering, typify, biometrics.

I. INTRODUCCIÓN

Actualmente se evidencia el aumento de delitos informáticos, debido en gran parte por la propagación de la pandemia Covid-19, lo que ha propiciado el incremento de las compras electrónicas, resulta de vital interés conocer cómo protegernos. Efectivamente los expertos en la materia informática pueden aprovecharse de ciertos métodos, herramientas, artificios para infiltrarse en sistemas informáticos de diversa índole. El empleo masivo de internet, medio por el cual viaja gran cantidad de información, ha generado dependencia, siendo de vital importancia proteger esta información de carácter altamente sensible tales como datos personales, económicos, políticos, tecnológicos, etc. Los delitos informáticos se cometen en el llamado espacio digital que trasciende fronteras, sin importar la ubicación para realizar el fraude informático, llegando mayormente el ciberdelincuente a quedar impune. De tal forma se ve la necesidad de regular expresamente estos delitos, por decirlo de alguna manera nuevos delitos.

Como consecuencia de la era digital, en la que la información es difundida enormemente por las redes telemáticas, los mecanismos empleados para acceder a estás, explotan vulnerabilidades, puesto que ningún sistema informático es infalible, es decir presenta errores tanto en su arquitectura como en su administración, soporte remoto, lo que conlleva a los nuevos ilícitos digitales en la comisión de fraudes y delitos informáticos, con mayor relevancia. Es así que las herramientas, tecnologías de la información, se pueden emplear para excelentes fines, pero lamentablemente también pueden perjudicar a terceros, como sustracción de patrimonios, diversos tipos de bienes, alterar, modificar, eliminar sistemas de seguridad, realizar infinitos tipos de fraudes; inclusive corromper los datos de entidades privadas y públicas. (Ortíz, 2013).

Su proceder del término phishing, está basado en la llamada ingeniería social. Dicha práctica se basa en la manipulación de las personas mediante técnicas psicológicas o habilidades adquiridas, propias de la naturaleza humana. En el phishing, se envían mensajes por medio del correo electrónico, ingeniosamente redactados solicitando información delicada. Por ejemplo, ponen la excusa de que necesitan actualizar datos personales de cuentas bancarias y los necesitan a la

brevedad. También pueden adjuntar archivos maliciosos en postales, recordatorios de cumpleaños, promociones, liquidaciones, etc; debe ser llamativo para ser descargado.

Por todo lo mencionado anteriormente, llegamos a la formulación del problema de la siguiente forma: ¿de qué manera el phishing vulnera la protección de datos personales en los delitos informáticos?

En cuanto a la justificación teórico - práctico, el problema de los delitos informáticos ha aumentado y se han desarrollado avanzados modos de operaciones electrónicas, complicados de descubrir, de cara a esta realidad es que el Derecho Penal se ha quedado plasmado en el tiempo, nuestro país no es la excepción, se han realizado modificaciones de manera genérica relacionado a los delitos informáticos, pero no basta. Hoy en día el phishing es el método de fraude online mayormente empleado; el cual emplea técnicas con la finalidad de manipular y engañar a las víctimas haciéndose pasar por entidades oficiales. Las técnicas consisten en apropiarse de información personal, como vienen a ser las credenciales o también datos de las cuentas y tarjetas de banca para la sustracción del dinero. Existen otras formas también empleadas como inducir a la víctima de manera que termine instalando un troyano, un malware o un ransomware, para luego pedir un rescate. Como justificación social, lo que se espera obtener con la presente investigación es generar una reforma legal en el cual se sancione la modalidad de phishing con una regulación expresa, porque en la realidad actual se requiere de una reforma legislativa para determinados casos que lo ameriten desde una posición nueva.

Por todo lo descrito, se estableció como objetivo general: Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos. En cuanto a los objetivos específicos, son: a) Explicar los alcances e impactos del phishing como apropiación de datos personales, b) Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad, y c) Analizar los presupuestos de los delitos informáticos en el código penal peruano.

II. MARCO TEÓRICO

Investigaciones realizadas en el exterior, reflejan los diversos tratamientos que le dan a esta nueva modalidad de cometer ilícitos penales. Por lo que, planteamos los siguientes, Devia (2017). en su tesis doctoral, tuvo como objetivo entregar una revisión sintética pero integral sobre los requisitos típicos del delito informático, permitiendo al lector tener una visión general, pero no por ello menos exhaustiva de este tipo de ilícito. Su diseño es descriptivo correlacional. La investigación culmina, obteniendo después de un riguroso análisis sobre el delito referente a estafa informática del artículo 248 numeral 2 del Código Penal Español, tratando reflejar a grandes rasgos sobre el fraude que se comete por medio de equipos de cómputo y sobre en qué tipo penal recae, estos ilícitos superan la soberanía de los Estados, reflejando un problema que atañe a todos los Estados. Así también Utreras (2017). en su tesis tuvo como objetivo demostrar la necesidad de tipificación del fraude informático en la ley chilena. Dicha investigación es de tipo descriptivo correlacional. Se llegó a la conclusión que el referido delito de fraude informático presenta características que imposibilitan incluirlo como parte de la estafa convencional, se recomienda tipificar en base a la dogmática y persecución criminal.

Desde nuestra realidad nacional mencionamos los siguientes, como el de Montoya (2017). en su trabajo de investigación, tuvo como objetivo determinar la importancia de la tipificación expresa del delito de clonación de tarjetas, para su adecuado tratamiento. Dicha investigación es de tipo cualitativa y se encuentra orientada a la comprensión de un fenómeno socio-jurídico. Los resultados obtenidos de la presente investigación demuestran la falta de claridad en relación con el delito sobre clonación de tarjetas, puesto que la ley lo abarca de manera general y genera confusión en cuanto a los delitos informáticos. Además, comenta Herrera (2018). en su tesis tuvo como objetivo general demostrar el nivel de eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017. La presente investigación es del tipo básico con un enfoque mixto. De los resultados obtenidos se concluyó que la ley de delitos informáticos que se administra en el referido distrito judicial de Huánuco es ineficaz, puesto que su tipificación es imprecisa, falta de implementación de la ley, no cuentan con logística ni instrumentos que se adecuen

a investigar, perseguir y sancionar este delito, lo cual deviene en imposible. Refiere Mengoa (2021). En su investigación, tuvo como objetivo determinar cómo el comportamiento del phisher-mule incurre en los delitos informáticos a la luz del Derecho Penal Peruano. Dicha investigación es de tipo básico de enfoque cualitativo. Se llegó a la conclusión que la conducta de phisher-mule no está individualizada en lo que respecta a su correcta la tipificación, se refiere de modo general que está relacionado con los delitos informáticos; siendo los (mule) los terceros involucrados, quienes retiran los montos productos del fraude en cuentas bancarias creadas previamente, para luego transferirlas a cuentas externas. Añade Díaz (2019). en su tesis tuvo como objetivo general determinar la eficacia de la ley Nº. 30096 - Ley de delitos informáticos respecto a su regulación en el derecho penal peruano. La presente investigación es de tipo básico con un enfoque cualitativo. De los resultados obtenidos se concluyó que en cuanto al tratamiento jurídico penal de los delitos informáticos es ineficaz, a razón de no contar con una fiscalía descentralizada que se encargue del tratamiento de esté lo cual deviene en una inseguridad jurídica, al no contar con la debida investigación a nivel preliminar. Finalmente concluye Rivero (2017). en su tesis, tuvo como objetivo analizar cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano. La presente investigación es de tipo Cualitativo aplicada. En los resultados, incide positivamente la admisión de evidencia digital, no tenemos una adecuada legislación de delitos informáticos referente a la cadena de custodia, así como manejarlo especialmente.

Respecto a las teorías y enfoques conceptuales, en principio debemos conceptualizar de forma general, qué es aquello que se ha denominado phishing. De tal forma, en las últimas décadas ha surgido una nueva forma de estafa, la cual consiste en *"Conducta delictiva diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños".* ABA (2020). Una vez obtenida la información esta es usada de modo fraudulento. La modalidad más empleada consiste en enviar gran cantidad de correos electrónicos, los cuales simulan pertenecer a entidades o empresas oficiales, siendo en realidad copias muy bien diseñadas que simulan ser

las legítimas, con la finalidad de obtener las credenciales. En resumen, obtener la mayor cantidad de datos de diversa índole para usarse de modo fraudulento. El phishing surgió a principios de los años noventa, siendo las primeras víctimas los clientes de America Online, el cual fue uno de los primeros proveedores de Internet. Un grupo de ciberdelincuentes llamados “Warez” cometieron fraudes, al inicio comercializaban software pirateado, luego generaban mediante unos algoritmos, números de tarjeta de crédito aleatorias para crear cuentas AOl y obtener provecho de los servicios. A raíz de lo sucedido la empresa America Online resolvió dicho problema. Finalmente, los delincuentes replicaron la página web AOL, haciéndose pasar como empleados enviando correos electrónicos, logrando obtener las credenciales de los usuarios. (Díaz, 2007).

Argumenta Cury (2011). En cuanto a la naturaleza jurídica no situamos en iter criminis; “*primero el sujeto idea el hecho punible, de modo que se representa intelectualmente la posibilidad de realización del mismo. Luego, si su voluntad acoge aquello que ha discurrido, el sujeto resuelve cometerlo, disponiéndose a planificar su conducta. Posteriormente, se dirige a preparar la ejecución del hecho punible, para lo cual ordena los medios e instrumentos para asegurar su éxito. Solo una vez que se encuentra en este punto se orientará a verificar la acción típica, o si se tratara de delitos de resultado, a causar el evento típico.* Para Novoa (2005). *“refiriéndose a aquel momento del desarrollo del delito en que se han producido todas las consecuencias del hecho delictuoso y en que el sujeto activo, por consiguiente, no sólo ha dado cima al hecho típico, sino ha logrado, además, obtener todos los efectos ilícitos que mediante él se proponía conseguir”.*

Para Montaperto (2018). sustenta que la conducta trata sobre un ataque informático, valiéndose de la ingeniería social, realizado por los llamados phishers que vienen a ser individuos con grado de conocimiento avanzado y experiencia en sistemas informáticos, cuyo fin es la obtención de información confidencial del victimario valiéndose del uso de engaño o ardid. Es evidente que constituye una actividad ilícita, pues la mayoría de los casos producen daños extrapatrimoniales y patrimoniales.

Sustentan Flórez & Díaz (2017). El ciberdelincuente se aprovecha de la poca pedagogía informática de los victimarios del phishing en las difusiones realizadas por pocas entidades financieras o estatales y de mínimo impacto social; puesto que la población que se ve afectada no suele ser parte de dichas campañas de prevención de dicho accionar. Aunado a ello, el poco conocimiento informático aumenta y en consecuencia esto genera pérdida de confianza por parte del consumidor en custodiar sus datos personales de naturaleza económica en el banco.

Sostiene Flores (2017). La justificación de individualizar el delito de phishing se basa en lograr la debida protección a bienes jurídicos tan relevantes como la intimidad y el patrimonio. Se deben establecer determinadas prevenciones con mayor énfasis en dichos bienes jurídicos, que por medios electrónicos son altamente vulnerados. Considera Calderón (2021). Quien pudiendo saber de qué trata el operativo o el delito, no disminuye ni elimina su culpabilidad, porque tienen conocimiento que su conducta es antijuridica, puesto que, a pesar de no saber, el pensar del sujeto en aquel momento, se concluye que su comportamiento incurre en conducta dolosa.

Comenta López (2014). refiere los distintos tipos de casos de phishing y distintos perfiles de víctimas. El más usual es el llamado deceptive phishing; el cual se da a través del correo electrónico, en la que se suplanta a una compañía reconocida para robar datos personales, como credenciales. Además, existe el malware-based phishing, el cual el correo tiene adjuntado un archivo malicioso o un enlace que al ingresar descarga e instala malware al aprovechar las vulnerabilidades del equipo del usuario. También Content-Injection phishing, en el cual se vale de que la página web no se encuentra actualizada, lo cual permite la inyección de código malicioso para obtener las credenciales. El Spear phishing, es similar el primer tipo descrito con la diferencia que está tiene conocimiento de lo que prefiere el cliente, valiéndose de detalles sofisticados muy persuasivos. Así también, el pharmin el cual ataca directamente al DNS, el cual es el intermediario entre el equipo solicitante y la página a visualizar; de tal forma que está visitando otra página distinta de la original, para obtener las credenciales. Otro tipo es el vishing en el

cual la forma de contacto es una llamada o un mensaje de voz. El smishing el cual se ejecuta vía SMS; el cual contiene términos alarmantes o muy atractivas para persuadir a las potenciales víctimas.

Sostiene Díaz (2020). Los ciberdelincuentes obtienen gran cantidad de usuarios por medio de chats, foros, comunidades, oportunidades laborales. Luego deben completar los campos con nombres completos y respectivas cuentas bancarias. Se comete el phishing enviando masivamente correos electrónicos que aparentan ser legítimos para luego solicitar las credenciales. Para conseguir extraer el dinero sin ser descubiertos emplean a los llamados mulas o que son los intermediarios, es la que se encarga de realizar las transferencias de dinero obtenida de forma ilegal en un mismo país, a otro usualmente países del este, lo cual dificulta la condena, donde radica el estafador, quedándose una pequeña compensación. El Phisher se vale de ofrecer puestos de trabajo desde casa al intermediario pues este muchas veces no tiene un trabajo estable, por lo tanto, debido a la necesidad acepta sin dudar. Es necesario señalar que en el mercado negro en inglés llamada “Deep Web”, se adquieren kits de phishing, en base a la compañía de ciberseguridad, en cuanto al precio en el año 2019 giraban en torno a los 300 dólares. En cuanto a los kits más básicos costaban desde 20 dólares. Así mismo los kits más avanzados bordeaban los 900 dólares. Dichos kits contienen herramientas complementarias informáticas con las cuales se gestiona el phishing. Usualmente contiene software de creación de páginas muy contundentes, así como también modelos de correos electrónicos; llegando los kits más avanzados unas listas de correos robados y programas automatizados que propagan el phishing a través de estos.

En ese sentido, existen Herramientas y técnicas de detección de phishing, mediante la introducción de la URL, es decir la dirección de la página web realizar un análisis de la página en mención, mostrándonos una aproximada probabilidad de ser maliciosa. Dichas páginas web poseen bases de datos altamente sofisticadas, contienen antivirus y motores de detección, por poner un ejemplo “VirusTotal”. Páginas como “URLScan”, adicionalmente no solo analiza la legitimidad de una dirección web, muestran detalles más a fondo, los cuales son esenciales de ser el caso para un análisis forense de una página web. También existen sitios web más

específico al phishing como “isitPhising”, el cual se vale de la inteligencia artificial, pues analiza, más de 40 características por página, así como ciertos patrones inteligentes basados en reglas heurísticas. Las direcciones web fraudulentas se parecen a las direcciones oficiales. Por ese motivo, en lo referente a su contenido y formato, presentan patrones y características parecidas. De igual forma sucede con los diseños de la página web, aunque sean de distintos kits de phishing, y se suplante a distintas empresas, siguen teniendo rasgos similares que diferencia a las páginas oficiales. Un modo de engañar es mediante la dirección web, es emplear letras parecidas, sustituir la ‘l’ por la ‘i’ mayúscula o inclusive ciertos caracteres cirílicos, árabes y hebreos para sustituir algunas letras romanas de esquema parecido, sustituir la letra ‘a’ en romano es idéntica a la ‘a’ en cirílico, pero Unicode las traduce a caracteres diferentes. Los phishers emplean como subdominio el dominio de la compañía legítima suplantada y completan la dirección web con alguna otra cadena, como ejemplo, “paypal.com.myaccount-cgibin.com”. Esta técnica es denominada combo-squatting. Respecto al impacto económico abarca tanto a los particulares, los primeros porque al obtener sus credenciales vacían su línea de crédito o transfieren, retirar el saldo disponible de ser tarjetas débito; y en segundo lugar el aspecto social afecta a las empresas, pues estas dejan de tener confianza con la banca, finalmente comienzan a tener menos fiabilidad. (Díaz, 2020).

Señala Eguiguren (2015). Su fundamento está claramente unido al acelerado progreso de la informática y las nuevas tecnologías para registrar, manejar y transmitir información en relación de datos personales, que requieren instituir ciertos niveles de control para salvaguardar estos datos personales, de igual forma proteger la privacidad y reserva ante su circulación y propagación en torno a terceros, mayormente incalculables. Aporta INCIBE (2016). La aplicación de la biometría en la actualidad presenta grandes beneficios y usos, en especial en lo relacionado con la seguridad informática, debido a que permite verificar la identidad del cliente por medio de mecanismos de autenticación como la identificación dactilar y facial, token digital vía sms.

Según Ford (2015). Surge en la modernidad otra línea de afectación, en cuanto se relaciona con el espacio digital llegando a afectar la esfera de la intimidad o las comunicaciones. Añade Arellano & Ochoa (2013). En cuanto al derecho a la intimidad debido al empleo de sistemas informáticos se han visto afectados. Por ello se ha visto la necesidad de proteger este bien jurídico, entendido como derecho a la intimidad informática, cuya particularidad radica en mantener en estricta reserva en las comunicaciones por medio de Internet.

En el año 2013 la Ley Nº 30096, “Ley de Delitos Informáticos”; fue creada con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. Al año siguiente sufrió una modificación por la Ley Nº 30171, siete artículos se modificaron para aclarar ciertas imprecisiones que difieren de la norma previa, y se tuvo que derogar el artículo 6, el cual trataba sobre el tráfico ilegal de datos. De lo cual se evidencia definiciones muy pobres, genéricas, que no son suficientes para delimitar en qué consiste el phishing. Respecto de los presupuestos de los delitos informáticos en el código penal peruano, el referido código establece en el Art. 154-A.- Tráfico ilegal de datos personales, y también en el Art. 196-A.- Estafa agravada inciso 5; los cuales generan ambigüedad, puesto que trata de manera general a los delitos informáticos y no permite una correcta delimitación del phishing.

De tal forma, señalamos que al momento de elaborar la Ley Nº 30096, se basaron en el “Convenio de Budapest”. Firmado en el 2001 y vigente a nivel internacional en el año 2004; en el cual participaron los países del Consejo de Europa “*con la finalidad de afrontar los delitos informáticos mediante mecanismos homologados de directrices de derecho penal parte sustantiva, así como establecer estándares en los procesos penales y participación trasnacional”.* En relación con este convenio, en el año 2019 el Poder Legislativo lo aprobó mediante su respectiva resolución y luego lo ratificó el mismo año por medio de decreto. Lo ideal hubiese sido emplearlo desde el año 2013, para una correcta utilidad por parte de los operadores de justicia y tomen conciencia de la gravedad de la vulneración de seguridad informática.

Por su parte tanto España, México y Argentina lo relacionan de manera general con su normativa penal. Siendo Colombia, la nación que ha incorporado la figura de suplantación de sitios web para capturar datos personales; la cual es la que más guarda relación con el delito de phishing, con una pena máxima de 8 años, a comparación de las demás naciones, es evidente que se ha tratado de ampliar la sanción por la gravedad del daño causado, al lucrar con los datos personales. En Estados Unidos está pendiente de aprobación un proyecto de Ley Federal que sanciona el phishing, mientras que en Chile no cuentan con normas que sancionen los delitos informáticos; por lo que se valen de la parte procesal, en cuanto a la aplicación de las técnicas generales.

III. METODOLOGÍA

3.1. Tipo y Diseño de Investigación

El tipo de investigación fue básico ya que se hizo un análisis solo de documentos mas no se efectuó una aplicación y no se utilizó estadística aplicada. De enfoque cualitativo, ya que se realizó un análisis de documentos y la técnica utilizada también incluyo la entrevista. (CONCYTEC, 2018).

El diseño de investigación es de tipo teoría fundamentada, porque se aportó nuevos puntos de vista, basada en la interpretación respecto de un ámbito determinado. (Hernández et al, 2014).

3.2. Categorías, Subcategorías y matriz de categorización

La primera categoría es phishing. Como subcategorías: Naturaleza jurídica, definiciones teóricas, tipos y clasificación. La segunda categoría es Delitos Informáticos. Como subcategorías: Naturaleza jurídica, modalidades. La matriz de categorización apriorística (Anexo Nº 01).

3.3. Escenario de estudio

El escenario de estudio abarcó todo el territorio peruano, pero en esencia el departamento y provincia de La Libertad, se obtuvo información de profesionales en Derecho también Ingenieros de Sistemas y se tuvo en consideración la documentación relacionada con el objeto de estudio de cómo se regula el phishing en la nación peruana.

3.4. Participantes

En la presente investigación participaron diez especialistas, de los cuales cinco son abogados especialistas en derecho penal y cinco son ingenieros de sistemas con un amplio conocimiento en sus respectivas especialidades. También se consideraron dos expedientes para el análisis.

3.5. Técnicas e instrumentos de recolección de datos

La técnica utilizada fue la entrevista no estructurada, la cual permitió obtener resultados que permitió relacionar las diversas posturas de los ingenieros de sistemas y abogados especialistas en materia penal a fin de verificar el problema planteado. Tuvo como instrumento la guía de entrevista, la cual

trató del documento donde figuran las respectivas interrogantes. También se empleó el análisis documental y su instrumento fue una ficha de recolección de datos. Fue una ficha en la que se extrajo datos importantes para analizar las categorías de estudios. (García, 2013).

3.6. Procedimiento

El procedimiento de la investigación constó de emplear la técnica de la guía de entrevista, también se empleó la ficha documental. Se analizó y se definió las categorías respectivas.

Primero se procesó los datos en una matriz, el cual tuvo la siguiente estructura: 1) Preguntas, 2) Entrevistado (Especialidad), 3) Respuestas, 4) Interpretación.

Segundo se procedió a la discusión de resultados obtenidos, se tuvo como base lo referido por los especialistas entrevistados, se consideró la relación con la normativa legal, el Código Penal, estudios anteriores y referencias bibliográficas.

En lo que respecta a la ficha documental, se empleó para conseguir información doctrinaria sobre el phishing y los delitos informáticos, luego se obtuvo resultados que fueron discutidos.

3.7. Rigor científico

Se ha cumplido con la rigurosidad científica ya que se validó el instrumento adoptado, pues antes de realizar la entrevista está fue revisada y validada por tres especialistas en la materia. También, se empleó las guías del método científico y las observaciones de los docentes metodólogos y especialistas en la materia. (Anexo Nº 03), de tal forma se cumple con lo requerido fiabilidad, pertinencia y veracidad para garantizar el rigor en la investigación (Izcara, 2014).

3.8. Método de análisis de datos

Respecto al método de análisis, se realizó un minucioso estudio de las entrevistas. Se empleó la codificación abierta, esto consistió en fracturar los datos y se obtuvo tanto ideas como sentidos y significados con la finalidad

de descubrir y desarrollar conceptos. En relación con Charmaz (2007). Los datos son segmentados, examinados y comparados en términos de sus similitudes y diferencias. Estas comparaciones deben quedar registradas en anotaciones que acompañan a cada código. Existen dos tipos de códigos la pre-codificación conceptualiza el fenómeno a través de la interpretación del analista y los in vivo son frases literales que expresan las palabras usadas por los individuos.

Se realizaron pasos inductivos, primero se puso los datos en categorías sin ningún tipo de condición previa. Se fijo un análisis paso a paso, de tal forma se realizó una aproximación de nivel microscópico.

3.9. Aspectos éticos

Se ha respetado la ética de las investigaciones ya que lo que se está describiendo, está citando, respetando sus ideas sin realizar un plagio. Se está respetando las citas con las normas apa, así mismo se ha utilizado un programa antiplagio para poder medir la originalidad del trabajo y también se está respetando el anonimato de los entrevistados. Existen tratados que protegen la originalidad de los autores, con mayor énfasis en la era de la globalización. (Frankel, 2015).

IV. RESULTADOS Y DISCUSIÓN

Se aplicó la guía de entrevista a los especialistas en ingeniería de sistemas y abogados del ámbito penal, siendo que, los entrevistados 1, 2, 3, 4 y 5 ingenieros especialistas que radican en la ciudad de Trujillo; también los entrevistados 6 y 7 abogados especialistas que radican en la ciudad de Trujillo; así mismo los entrevistados 8, 9 y 10, abogados especialistas que radican en la ciudad de Lima.

Dentro del proceso de desarrollo de la presente tesis a fin de dar cumplimiento a los objetivos específicos, se obtuvieron los siguientes resultados:

OBJETIVO ESPECÍFICO Nº 1: Explicar los alcances e impactos del phishing como apropiación de datos personales

TABLA 1: Respuesta de los especialistas respecto de la pregunta 1 de la entrevista

¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Ingeniero 1	Lograr que estos les envíen datos confidenciales (información considerada como sensible) con la finalidad de obtener un beneficio económico de estos y a través de estos, ocasionando en los usuarios estafados desde el hurto (delito contra el patrimonio) hasta la utilización de sus cuentas y equipos (robo de identidad) para otras actividades delictivas que pueden ser de la misma índole o no.	Obtener beneficios económicos producto de los datos personales.	No se encontraron divergencias.
Ingeniero 2	El único peligro y fatal para la víctima es la violación a su información confidencial, el cual tiene valor constitutivo de su privacidad.	Obtener beneficios económicos producto de los datos personales.	No se encontraron divergencias.
Ingeniero 3	Los ciberdelincuentes pueden utilizar la información personal robada mediante phising para distintos fines como: suplantación de identidad, robo de dinero en bancos, espionaje y utilización de las cuentas robadas para fines delictivos.	Obtener beneficios económicos producto de los	No se encontraron divergencias.

		datos personales.	
Ingeniero 4	Usurpación de identidad informática, utilizan datos personales y credenciales de cuentas para ser usados de forma maliciosa.	Obtener beneficios económicos producto de los datos personales.	No se encontraron divergencias.
Ingeniero 5	Adquisición de servicios, algunos bienes o realización de transacciones no autorizadas que pueden terminar incluso en el robo de dinero en las cuentas personales o de la empresa.	Obtener beneficios económicos producto de los datos personales.	No se encontraron divergencias.
Resultado	Los cinco entrevistados consideran que los peligros a los que son expuestos los datos personales en el delito de phishing son de obtener beneficios económicos producto de la información personal obtenida.		

Fuente: La tabla de entrevista que obra en anexo 05.

TABLA 2: Respuesta de los especialistas respecto de la pregunta 2 de la entrevista

¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Ingeniero 1	La responsabilidad de la banca online, la cual debe de ser tomada como de naturaleza casi objetiva, derivada de la exigencia a la entidad titular del servicio de adoptar medidas de seguridad necesarias y renovables ante los distintos modos de fraude informático, de tal modo que, salvo que se acredite la negligencia grave por parte del usuario de la banca electrónica, la entidad financiera debe responder del reintegro de los importes obtenidos de forma fraudulenta.	La entidad bancaria es responsable, salvo se acredita responsabilidad del usuario.	
Ingeniero 2	En toda medida, las financieras deben garantizar y ser responsables de la seguridad de la información de todos sus clientes. Actualmente, se cuenta con la tecnología para rastrear las operaciones o transacciones.	La entidad bancaria es responsable.	

Ingeniero 3	Cada vez que se brindan datos personales a una empresa, como un banco, se encuentran en la obligación de informar a sus clientes la finalidad con la que será usada esta información, de esta forma se está asegurando la protección de la misma respecto a fines distintos a los acordados.	La entidad bancaria es responsable.	
Ingeniero 4	No es 100%, solo registran las transacciones; ahora si desean proteger sus tarjetas piden una comisión o pago mensual, pero aun así no apoyan al 100%.		La entidad bancaria no es totalmente responsable.
Ingeniero 5	Los bancos y cualquier empresa que nos provee de algún servicio donde se almacenan nuestros datos debe tomar conciencia de que son los responsables de esos datos y contratar especialistas que permitan asegurar que no sean difundidos por un ataque informático y sobre todo, prevenir el caso de convenios con terceros para la adquisición de nuevos productos a través de terceros.	La entidad bancaria es responsable.	
Resultado	A excepción del entrevistado 4, todos los demás consideran que la entidad bancaria es totalmente responsable de proteger los datos personales. Adicionalmente el entrevistado 1 considera que, salvo se acredite responsabilidad del usuario, la entidad bancaria es responsable.		

Fuente: La tabla de entrevista que obra en anexo 06.

TABLA 3: Respuesta de los especialistas respecto de la pregunta 3 de la entrevista

¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Ingeniero 1	A la entidad le corresponde capacitar y evaluar de manera constante al personal que tiene a su cargo referidos al área de Tecnologías de la Información acerca de las amenazas existentes y conforme vayan apareciendo referidas al fraude informático de este tipo. Así mismo, iniciar de manera conjunta con otros bancos por medio de las asociaciones existentes, o de manera individual, campañas mediáticas que informen y ayuden a implementar una cultura de prevención en sus clientes acerca de los cuidados que deben de tener con respecto al Phishing.	Capacitación del personal, campañas mediáticas respecto al phishing.	No se encontraron divergencias.

Ingeniero 2	Deben emplear, todos los mecanismos básicos pero seguros que garanticen la confiabilidad, la integridad y la disponibilidad de la información al realizar las operaciones, en los trabajos de: Autenticación, Detectivos y Correctivos.	Capacitación del personal.	No se encontraron divergencias.
Ingeniero 3	Los bancos sólo pueden optar por hacer campañas de concientización para informar a sus clientes sobre el adecuado uso de sus plataformas y funcionamiento de sus medios de comunicación. Por el lado de los clientes, informarse sobre el tema, tomar tests y reforzar la seguridad de su ordenador con un antivirus, sistema operativo y navegadores actualizados.	Campañas mediáticas respecto al phishing, cultura de prevención por parte de los clientes.	No se encontraron divergencias.
Ingeniero 4	Los mecanismos de seguridad del banco son constantes, pero no ayudan al 100%. Los clientes son la clave de proteger sus credenciales, utilizando una red privada y utilizar su propio equipo informático posible o mayor seguridad posible.	Capacitación del personal, cultura de prevención por parte de los clientes.	No se encontraron divergencias.
Ingeniero 5	Fundamentalmente contratar servicios especializados para evitar el ataque informático y por ende el robo de la información personal del usuario, un buen data center, por ejemplo.	Capacitación del personal.	No se encontraron divergencias.
Resultado	Los cinco entrevistados consideran que los mecanismos a emplear para prevenir el delito de phishing consisten en capacitación del personal, también realizar campañas mediáticas a fin de que los clientes cuenten con una cultura de prevención.		

Fuente: La tabla de entrevista que obra en anexo 07.

OBJETIVO ESPECÍFICO Nº 2: Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad

TABLA 4: Respuesta de los especialistas respecto de la pregunta 4 de la entrevista

¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Abogado 1	Castigado por el delito de tráfico ilícito de datos, castigando a quien atente contra la intimidad, sirviendo como consecuencia de la violación a la intimidad	Inmerso en los delitos informáticos	No se encontraron divergencias.

Abogado 2	El código penal peruano en su art. 154 refiere la protección del derecho a la intimidad; sin embargo, al emplear medios electrónicos el delito de phishing está inmerso en la ley de Delitos Informáticos, la cual protege información confidencial que vulnera la intimidad.	Inmerso en los delitos informáticos	No se encontraron divergencias.
Abogado 3	El CP protege a la persona que son víctimas del phishing mediante los delitos informáticos a fin de que no sean vulnerados su intimidad o privacidad.	Inmerso en los delitos informáticos	No se encontraron divergencias.
Abogado 4	El Código Penal, de acuerdo con la tutela de derechos otorgados por el Estado, no detalla con precisión la protección ante el delito de phishing, dejando acción al conocimiento y diligencia del titular del bien.	No detalla con precisión la protección ante el delito de phishing	No se encontraron divergencias.
Abogado 5	El Código Penal en su Art. 154 protege el derecho a la intimidad el cual tiene una relevancia constitucional, sin embargo, al emplear un equipo de cómputo para el acceso de datos estos se encontrarían inmersos en la Ley de Delitos Informáticos (Ley Nº 30096) la cual protege la interceptación de datos informáticos específicamente de datos personales o situaciones personales que atenten contra la intimidad.	Inmerso en los delitos informáticos	No se encontraron divergencias.
Resultado	Los cinco entrevistados consideran que la protección del derecho a la intimidad en el código penal en cuanto al delito de phishing, al emplear medios electrónicos, están inmersos en los delitos informáticos.		

Fuente: La tabla de entrevista que obra en anexo 08.

TABLA 5: Respuesta de los especialistas respecto de la pregunta 5 de la entrevista

¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Abogado 1	La normativa es eficaz, la desventaja es la falta de información por parte de los usuarios de internet que al no conocer la normativa no hacen su denuncia a tiempo	Normativa eficaz, usuarios les falta información	
Abogado 2	En el art. 154 del código penal peruano se estipula el derecho a la intimidad personal o familiar, donde se advierte que quien viola dicho derecho valiéndose de		Normativa ineficaz

	instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de la libertad no menor de 2 años, lo cual es muy básico y no es más que un susurro amedrentamiento a una acción delictiva delicada dado que como todos sabemos una pena de no más de 2 años es una pena sin efectividad de cárcel o cumplimiento de la misma, por lo que no se protege en si en fin de cuentas el derecho a la libertad por la poca severidad del castigo impuesto.		
Abogado 3	Todos los países tienen buenas normas solo es que deben aplicarse y hacer valer sus derechos, en nuestro caso la norma es eficaz sin embargo algunos abogados creen que los delitos informáticos solo protegen sobre la máquina y no saben que lo que protegen es la intimidad de su contenido que se vulnera o rompe su clave para introducirse y viene	Normativa eficaz, abogados les falta capacitación	
Abogado 4	Como tal para el delito de phishing, no está taxativamente definido.		Normativa ineficaz
Abogado 5	Debido a su gran variedad y especialidad, la tarea de tipificación de los delitos informáticos resulta una labor muy complicada, por lo que se hace necesario delimitar con mucha precisión las características adecuadas de la criminalización de estas conductas y, por, sobre todo, el bien jurídico afectado como base de la sistematización. El Derecho Penal sanciona a quien intercepta de manera indebida información sensible en un sistema informático, que podría ser la identidad de sus miembros, referencias personales, números de cuentas bancarias, datos que en manos extrañas podrían causar graves daños económicos y morales, en líneas generales el delito de interceptación de datos informáticos busca evitar el uso abusivo de los medios informáticos, específicamente la divulgación y trasmisión de datos o situaciones personales que atenten contra la intimidad personal.	Normativa eficaz	
Resultado	Los entrevistados 1, 3 y 5 consideran que la normativa es eficaz; sin embargo, los entrevistados 2 y 4 opinan que la normativa es ineficaz por la poca severidad del castigo impuesto y por no estar taxativamente definido.		

Fuente: La tabla de entrevista que obra en anexo 09.

TABLA 6: Respuesta de los especialistas respecto de la pregunta 6 de la entrevista

¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Abogado 1	Pueden ser sujetos a hurto, extorsión, y demás delitos que atenten contra la intimidad	Comisión a otros delitos	No se encontraron divergencias.
Abogado 2	La persona sufre la violación de un derecho propio como el de la intimidad personal y familiar, lo cual muchas veces acaba en la comisión de otros delitos como la extorsión, la estafa, violación de derechos de autor, suplantación de identidad, etc.	Comisión a otros delitos	No se encontraron divergencias.
Abogado 3	Lo que se protege es su intimidad cuando se introducen rompiendo su clave, lo que suceda internamente en esa máquina nos conlleva a otros delitos es decir la máquina es el medio.	Comisión a otros delitos	No se encontraron divergencias.
Abogado 4	La afectación es de carácter patrimonial definitivamente puesto que el autor material se apodera de los datos para conseguir un beneficio material. Los daños colaterales o consecuentes también pueden afectar a la intimidad	Comisión a otros delitos	No se encontraron divergencias.
Abogado 5	Los datos personales e íntimos de las personas en manos extrañas podrían causar graves daños económicos y morales, específicamente la divulgación y trasmisión de datos o situaciones personales que atenten contra la intimidad personal.	Comisión a otros delitos	No se encontraron divergencias.
Resultado	Los cinco entrevistados consideran que la afectación personal acarrea en la comisión de otros delitos.		

Fuente: La tabla de entrevista que obra en anexo 10.

OBJETIVO ESPECÍFICO Nº 3: Analizar los presupuestos de los delitos informáticos en el código penal peruano

TABLA 7: Respuesta de los especialistas respecto de la pregunta 7 de la entrevista

¿Considera que la vigente Ley Nº 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**

Abogado 1	La ley tiene que sufrir modificación y adaptarse a la realidad actual, pues cambió mucho la sociedad después del Estado de emergencia	Necesaria modificación de la normativa	
Abogado 2	Si es deficiente, dado que si así no fuera no se daría la Violación del secreto de las comunicaciones. Interceptación de comunicaciones personales de manera ilegal, utilización y modificación de los datos de carácter personal sin consentimiento, acceso ilegal a datos y sistemas informáticos.	Necesaria modificación de la normativa	
Abogado 3	No es deficiente, sino hay que saber utilizarla y aplicarla que únicamente y exclusivamente es el medio para cometer otros injustos penales.		Saber utilizarla y aplicarla
Abogado 4	Le falta mayor precisión, se hace necesario una nueva implementación normativa al respecto sobre todo en esta coyuntura actual donde este tipo de delitos se han incrementado.	Necesaria modificación de la normativa	
Abogado 5	No es deficiente, lo que se necesita es un control en torno al acceso de los datos personales y la venta de los mismos por sujetos inescrupulosos.		Saber utilizarla y aplicarla
Resultado	Los entrevistados no responden con precisión a la pregunta planteada; sin embargo, se tiene que, los entrevistados 1, 2 y 4 consideran que es necesaria la modificación de la normativa, sin embargo, los entrevistados 3 y 5 opinan que no es deficiente, solo es necesario saber utilizarla y aplicarla.		

Fuente: La tabla de entrevista que obra en anexo 11.

TABLA 8: Respuesta de los especialistas respecto de la pregunta 8 de la entrevista

¿Sería pertinente la creación de nuevos tipos penales? Explique			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Abogado 1	Si, porque ha evolucionado la utilización de medios electrónicos, sobre todo en la administración publica	Si, por la ciberdelincuencia	
Abogado 2	Sí, todo en el derecho es renovable y mejorable; y en cuanto a nuevos tipos penales sería bueno que esto abarque des una pena privativa de libertad más severa hasta la complicidad y actuación en banda o como organización criminal a quien actúen en conjunto aprovechando de sus conocimientos técnicos en la materia, inclusive el retiro o cese de algún estudio superior	Si, por la ciberdelincuencia es necesaria la tipificación con sus respectivas agravantes.	

	en la materia como consecuencia de su inequívoca utilización de ello en fines delictivos.		
Abogado 3	No necesariamente, está bien definido en la norma penal. Cuando se comete este injusto penal lo que sucede es saber utilizarla y conectarla con otros delitos que se cometen, que serían un concurso ideal de delitos		No, saber utilizarla y conectarla con otros delitos que se cometen
Abogado 4	Desde luego que es muy pertinente la creación de nuevos tipos penales considerando que la capacidad operativa de la ciber delincuencia se nutre de la tecnología, por tanto, es necesaria una nueva calificación típica y sus agravantes por la naturaleza misma del ilícito penal.	Si, por la ciberdelincuencia es necesaria la tipificación con sus respectivas agravantes.	
Abogado 5	Como sabemos el Derecho Penal debe ser la última ratio, motivo por el cual no debe ser utilizado en todo proceso de criminalización, debiendo echar mano o crear otros medios de control social que tengan una relevancia menos gravosa y pueda controlar todo el tráfico de la información de datos relacionados a ordenadores informáticos.	Si, por la ciberdelincuencia es necesaria la tipificación con sus respectivas agravantes.	
Resultado	A excepción del entrevistado 3, todos los demás consideran que sí es necesaria la creación de nuevos tipos penales; sin embargo, el entrevistado 3 opina que no es necesario, porque solo basta saber utilizarla y conectarla con otros delitos que se cometen.		

Fuente: La tabla de entrevista que obra en anexo 12.

TABLA 9: Respuesta de los especialistas respecto de la pregunta 9 de la entrevista

¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Abogado 1	No, porque este delito siempre es doloso, no hay culpa, siempre es doloso.	Delitos dolosos	No se encontraron divergencias.
Abogado 2	Así es, toda acción dolosa es un plus de consideración agravante, es menester que los delitos de phisher puedan formar parte ya los delitos informáticos y sus extensiones.	Delitos dolosos	No se encontraron divergencias.
Abogado 3	En principio todo delito tiene autores y coautores son los hechos que van a demostrar la participación de cada uno de los agentes, dado que toda violación a cualquier norma	Delitos dolosos	No se encontraron divergencias.

	penal, el órgano jurisdiccional debe identificar a estos agentes.		
Abogado 4	Considero que sí, definitivamente son delitos dolosos y sobre todo que se aprovechan de la confianza de la víctima para ocasionar el daño.	Delitos dolosos	No se encontraron divergencias.
Abogado 5	El phisher es el autor directo y la gravosidad del hecho se debe tener en cuenta con relación al daño ocasionado, teniendo en cuenta el sentido de la proporcionalidad de la pena.	Delitos dolosos	No se encontraron divergencias.
Resultado	Los cinco entrevistados consideran que el phishing es un delito eminentemente doloso.		

Fuente: La tabla de entrevista que obra en anexo 13.

ANÁLISIS DOCUMENTAL: En cuanto al análisis documental, se obtuvo dos casos. El primero de la nación de Colombia y el segundo de nuestra nación. Ambos tienen la calidad de Casación y están relacionados con mi tema de investigación. Estos documentos aportaran al apartado de Discusión de Resultados.

Figura 1. Síntesis de Casación 18614—2016—Colombia

COLOMBIA – 18614 – 2016	
HECHOS	**FUNDAMENTOS**
Se sustrajo de la cuenta afectada a once cuentas pertenecientes a clientes del mismo banco. En la primera fecha $84'590.000 y $40'000.000 en la segunda. El ingeniero encargado por el Banco para esa labor, le informo a la demandante que el fraude se realizó bajo la modalidad de phishing o spoofing. Los once destinatarios de las transferencias retiraron los dineros abonados a sus cuentas en sucursales de las ciudades de Barranquilla y Santa Marta.	Los empleados señalan que recibieron un aviso que indicaba que el acceso estaba bloqueado por 12 horas. No era algo extraño porque ya había ocurrido con antelación sin repercusiones. La "página web con la cual se comete el engaño o phising es completamente idéntica a la página suministrada por el banco, por lo cual no es posible para un usuario normal identificar dicho engaño". Si la sustracción no fue el resultado de una actuación culposa del cliente, quiere decir que cualquiera pudo ser víctima, y era un deber inexcusable de la entidad financiera precaverlo.

Figura 2. Síntesis de Casación 956—2017—Perú

PERÚ – 956 – 2017	
HECHOS	**FUNDAMENTOS**
El Gerente de Transportes Chiclayo Sociedad Anónima, se percata que todo el dinero (US$.125,000.00), había sido hurtado. El Banco demandado no había brindado ni recomendado la seguridad que el caso requería. Dichas operaciones no habían sido autorizadas por el Director Gerente de la empresa. El Banco Continental Sucursal Chiclayo incurrió en culpa inexcusable, por su negligencia grave no brindó a la empresa demandante las garantías requeridas para la realización de sus movimientos económicos a través del Sistema Continet.	Si la demandante se ha visto sorprendida por alguna técnica de estafa electrónica conocida como phising, troyanos, pharming, entre otras, es culpa única y exclusiva de la empresa demandante por no tomar las medidas de seguridad que el caso ameritaba. El Gerente demandante era el único conocedor de los códigos y claves para realizar operaciones electrónicas, no se advierte un actuar antijurídico de la empresa demandada, que establezca que incurrió en culpa inexcusable. Dicho banco prestó las medidas de seguridad que pudo prevenir el hecho delictivo; por lo que, no concurre el elemento de la antijuricidad para la atribución de responsabilidad. La empresa demandante sufrió un robo cibernético, conforme el expediente penal número 7061-2008, el Banco Continental no tiene responsabilidad alguna de carácter penal (reafirma la inexistencia de la antijuricidad). El banco, facilitó a la fiscalía el IP para determinar el lugar, hora y fecha del hecho delictivo, se trata de una banda delincuencial y que los retiros dinerarios se dieron en la ciudad de Lima. Recayendo, tal responsabilidad en Tomás Alberto Pesaque Benavides. La imputación a la entidad bancaria no ha sido corroborada o acreditada con documentos o pericias que determinen la responsabilidad de dicho delito de hurto agravado sea del demandado; las pretensiones de lucro cesante y daño emergente que se alegan, tampoco han sido acreditadas.

En el presente acápite relacionado a la discusión de resultados se procederá a redactar el resultado obtenido del método de triangulación, en relación con la información obtenida de instrumentos de recolección de información, análisis documental, antecedentes de la investigación e información doctrinaria, en el contexto siguiente:

La presente investigación tuvo como objetivo general **Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos;** dentro del cual se plantearon los siguientes objetivos.

Respecto al **objetivo específico Nº 1:** explicar los alcances e impactos del phishing como apropiación de datos personales, se plantearon las siguientes interrogantes:

1.- ¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?
2.- ¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?
3.- ¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?

Se obtuvo los siguientes resultados, en la tabla Nº1 que obra en las líneas precedentes; en tanto, la totalidad de los entrevistados señalan que los ciberdelincuentes al apropiarse de los datos personales lucran producto de estos; lo cual guarda relación con Utreras (2017), quien refiere que esté delito no calza como parte de la estafa convencional, por su propia naturaleza; así también con Montaperto (2018), quien sustenta que en mayor parte causan daños extrapatrimoniales y patrimoniales; criterio que compartimos, por cuanto los responsables de estos nuevos delitos se valen del poco conocimiento de las víctimas para causar graves daños de diversa índole.

Continuando con el análisis del primer objetivo, en la tabla Nº2; la mayoría de los entrevistados señalan que la entidad bancaria es la responsable de proteger los datos personales; sin embargo, también se considera que es posible

acreditar responsabilidad del usuario, lo cual guarda relación con Mengoa (2021), quien señala que no se debe permitir que cualquier persona obtenga cuentas bancarias, sin pasar por un determinado filtro; así también con Díaz (2020), quien señala que la banca se ve afectada socialmente pues estas empiezan a tener menos confianza y fiabilidad; criterio que compartimos, por cuanto esto genera desconfianza por parte de los usuarios, al no sentirse seguros de salvaguardar sus datos personales.

De acuerdo con la tabla Nº3, la mayoría de los entrevistados señalan que los mecanismos a emplear consisten en capacitación del personal y campañas mediáticas que generen cultura de prevención, lo cual guarda relación con INCIBE (2016), quien refiere que la biometría en la actualidad presenta grandes beneficios y usos, debido a que permite verificar la identidad del cliente por medio de mecanismos de autenticación como la identificación dactilar y facial, token digital vía sms; así también con Flórez & Díaz (2017), quienes señalan que el ciberdelincuente se vale de la poca pedagogía tecnológica en lo referido a las pocas campañas bancarias preventivas; criterio que compartimos, por cuanto dichas campañas al tener poca afluencia, no genera el impacto deseado; por lo cual es necesario informarse de las nuevas formas delictivas, puesto que, al obtener nuestros datos personales, estos pueden ocasionar pérdidas materiales, así como también derivar en la comisión de otros delitos. Con lo cual damos por logrado el presente objetivo.

Respecto al **objetivo específico Nº 2:** explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad, se plantearon las siguientes interrogantes:

4.- ¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?

5.- ¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?

6.- ¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?

Se obtuvo los siguientes resultados, en la tabla Nº4 que obra en las líneas precedentes; en tanto, la totalidad de los entrevistados señalan que, al emplear medios electrónicos, en protección del derecho a la intimidad en el código penal en relación al delito de phishing, están inmersos en los delitos informáticos; lo cual guarda relación con Devia (2017), quien refiere que esté delito informático al emplear equipos de cómputo sobrepasa la soberanía de los Estados; así también con Eguiguren (2015), quien sostiene que debido al acelerado progreso de la informática es necesario establecer ciertos niveles de control para poner a buen recaudo los datos personales; criterio que compartimos, por cuanto se requiere emplear los medios informáticos necesarios para proteger el derecho a la intimidad; el cual se ve vulnerado por personas inescrupulosas con avanzados conocimientos informáticos, por cuanto se debe garantizar la seguridad que guarda relación con la protección del derecho a la intimidad al emplear dispositivos electrónicos; puesto que se puede y debe hacer buen uso de la tecnología.

Continuando con la discusión, en la tabla Nº5 tres de los entrevistados señalan que la normativa es eficaz, sin embargo, dos de los entrevistados opinan que es ineficaz, justificándose en la poca severidad de la pena y de no estar taxativamente definido, lo cual guarda relación con Herrera (2018), quien sostiene que la tipificación de los delitos informáticos es imprecisa; así también con Arellano & Ochoa (2013), quienes argumentan la necesidad de proteger esté bien jurídico, llámese intimidad informática, la cual debe tener absoluta reserva en lo relativo a la comunicación virtual; criterio que compartimos, por cuanto la normativa es ineficaz, puesto que no guarda relación con la sanción impuesta, tal como se aprecia en la Casación N° 956-2017 Lambayeque, en la cual se tuvo la debida diligencia, al ser el gerente general el único conocedor de los datos personales para realizar operaciones electrónicas; y esté alega culpa inexcusable por parte de la entidad bancaria, en la presente casación, no se contó con la debida motivación puesto que dicha conducta no se encuentra

tipificada; por lo mencionado, es necesario tipificar el phishing con sus respectivas delimitaciones.

De la tabla Nº6 la totalidad de los entrevistados señalan que la forma en la que se ve afectada la persona acarrea en la comisión de otros delitos, lo cual guarda relación con Flores (2017), quien señala que se basa en proteger bienes jurídicos de alta relevancia como la intimidad y el patrimonio; así también con Ford (2015), quien señala que, al relacionar el espacio digital, esté llega a afectar la esfera de la intimidad y también las comunicaciones; criterio que compartimos, por cuanto las víctimas no solo pierden sus datos personales, sino que también sufren más daños relativos a su intimidad y al patrimonio, producto de lucrar con los datos personales a costa de la persona afectada. Con lo cual damos por logrado el presente objetivo.

Respecto al **objetivo específico Nº 3:** analizar los presupuestos de los delitos informáticos en el código penal peruano, se plantearon las siguientes interrogantes:

7.- ¿Considera que la vigente Ley Nº 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?
8.- ¿Sería pertinente la creación de nuevos tipos penales? Explique
9.- ¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?

Se obtuvo los siguientes resultados, en la tabla Nº7 que obra en las líneas precedentes; en tanto, la mayoría de los entrevistados señalan que, es necesaria la modificación de la normativa; sin embargo, dos de los entrevistados opinan que solo se ve la necesidad de saber utilizarla y aplicarla; criterio que no compartimos, por razón de Rivero (2017), quien refiere que no tenemos una adecuada legislación de delitos informáticos; así también con López (2014), quien refiere los distintos tipos de casos de phishing, los cuales emplean términos muy alarmantes para captar potenciales víctimas; por cuanto la normativa debe ser modificada, tal como se aprecia en la Casación Nº 18614-

2016 Colombia, en la cual no se probó responsabilidad de la víctima, puesto que el cliente no participó de ninguna transacción, siendo la responsabilidad de los empleados de la entidad bancaria; la corte no llegó a casar la sentencia previa, que establecía la responsabilidad de la entidad bancaria; por cuanto es necesario tipificar el phishing con sus respectivas delimitaciones.

De la tabla Nº8 la totalidad de los entrevistados señalan que, es necesaria la creación de nuevos tipos penales; sin embargo, uno de los entrevistados opina que solo se ve la necesidad de saber utilizarla y conectarla con otros delitos que se comenten; criterio que no compartimos, por razón de Montoya (2017), quien refiere que la ley abarca de manera general lo cual genera confusión en cuanto a los delitos informáticos; así también con Cury (2011), quien refiere que se trata de un delito de resultado; así también con Díaz (2019), quien señala que no se cuenta con una fiscalía descentralizada que, dé el tratamiento debido, lo cual deviene en inseguridad jurídica, puesto que no es posible una adecuada investigación a nivel preliminar; por cuanto es necesario la creación de nuevos tipos penales, por la ciberdelincuencia, la cual aumentó después del Estado de Emergencia.

De la tabla Nº9 la totalidad de los entrevistados señalan que el phishing es un delito eminentemente doloso, lo cual guarda relación con Calderón (2021), quien refiere que incurre en conducta dolosa al tener conocimiento de que trata el operativo, razón por la cual su conducta es antijurídica; así también con Novoa (2005), quien señala que consiste en la obtención de todos los efectos ilícitos que mediante él se proponía conseguir; criterio que compartimos, por cuanto siempre existe dolo en esté delito, también sufren en gran medida daños relativos a su intimidad y patrimonio. Con lo cual damos por logrado el presente objetivo.

V. CONCLUSIONES

El phishing vulnera la protección de datos personales en los delitos informáticos, debido al empleo generalizado de la ingeniería social; siendo muchas veces complicado identificar a los participantes del delito informático, puesto que los ciberdelincuentes se aprovechan de conocimientos técnicos, generan daños patrimoniales, así como también afecta la intimidad, se debe actualizar la normativa vigente, pues la sociedad lo refleja luego del estado de emergencia.

Los alcances e impactos del phishing como apropiación de datos personales, radica en base a la jurisprudencia, la doctrina, en obtener información confidencial de la víctima mediante el uso de engaño o ardid, se aprovechan de la poca pedagogía informática. Además, señalan respecto de los mecanismos de autenticación a emplear, como identificación dactilar y facial, token digital por mensaje de texto, de tal forma se busca generar una cultura de prevención por parte de los clientes, así también la debida capacitación por parte del personal de la banca.

La importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad, según los doctrinarios, radica en la necesidad de establecer ciertos niveles de control, por parte de la entidad bancaria, para poner a buen recaudo los datos personales, también llamado intimidad informática, resguardando la seguridad del derecho a la intimidad al emplear dispositivos electrónicos.

Los presupuestos de los delitos informáticos en el código penal peruano se sancionan con el Art. 154-A.- Tráfico ilegal de datos personales, y también en el Art. 196-A.- Estafa agravada inciso 5; los cuales generan ambigüedad. Así también con la Ley Nº 30096, “Ley de Delitos Informáticos”, el cual en su inciso 9º “El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral”. Dichos presupuestos son definiciones muy genéricas, que no son suficientes para delimitar en qué consiste el phishing. Además, los especialistas refieren que se tratan de delitos eminentemente dolosos.

VI. RECOMENDACIONES

Se sugiere verificar que se encuentra en un canal seguro, puesto que las empresas oficiales solo emplean “HTTPS”, como certificado de seguridad. En caso de duda puede contactar a la entidad emisora del supuesto mensaje de texto, correo electrónico, llamada telefónica, página web, etc., de tal forma evitará verse perjudicado.

Se recomienda a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, implementar mecanismos de autenticación como identificación dactilar y facial, token digital por mensaje de texto, de tal forma el personal debe estar altamente capacitado y por parte de los usuarios no confiar en supuestas promociones, ofertas, todo tipo de liquidaciones, etc., ya que la mayoría de las veces está visualizando sitios web casi idénticos a los oficiales, de esta manera se fomenta una cultura de prevención.

Se recomienda al Congreso de la República, actualizar la normativa vigente con relación a los Delitos Informáticos, puesto que estos nuevos delitos se han incrementado, ya que el estado de emergencia nos sigue afectando, además estos nuevos delitos tienen mayormente sanciones no efectivas, lo cual muchas veces causa que el ciberdelincuente quede libre; debido a los beneficios que otorga la ley al confesar el delito.

Se recomienda al Congreso de la República, ampliar y profundizar la redacción que comprende los delitos informáticos; mediante términos técnicos más específicos, los cuales permitirán prevenir y sancionar estos nuevos delitos, como el delito de phishing, por lo que se debe comparar y analizar con el Derecho Penal Colombiano ya que estos, han incorporado la figura suplantación de sitios web para capturar datos personales; la cual guarda relación con el delito de phishing, de igual forma, la debida capacitación al personal que labora en las fiscalías para la correcta investigación y sanción de los ciberdelincuentes.

REFERENCIAS

ABA. (2020). Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce (19 de abril del 2021). *AMERICAN BAR ASSOCIATION (ABA)-Rule of Law Initiative. Proyecto de Apoyo al Sector Justicia. Taller de Investigación Criminal y Litigación Oral Especializado en Delitos Informáticos- Cybercrime (diapositiva).* https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/

Arellano, W., & Ochoa, A. (2013). *Derechos de privacidad e información en la sociedad de la información y en el entorno TIC.* Lima: Revista IUS.

Aguilar, C (2008). *Delitos patrimoniales*. Santiago: Metropolitana.

Baena, G. (2007). *Metodología de la investigación*. México: Publicaciones Cultural.

Charmaz, K. (2007). *Constructing grounded theory. A practical guide through qualitative analysis.* Thousand Oaks, CA: Sage.

Contreras, A. (2009). *Metodología de la investigación*. México: Editorial ST.

CONCYTEC (2018). *Reglamento de calificación, clasificación y registro de los investigadores del sistema nacional de ciencia, tecnología e innovación tecnológica – Reglamento RENACYT.* (24 de mayo del 2021). https://portal.concytec.gob.pe/images/renacyt/reglamento_renacyt_version_final.pdf

Ministerio de relaciones exteriores (2019). *Convenio sobre la ciberdelincuencia: Budapest, 23.XI.2001. Serie de Tratados Europeos - N° 185.* (17 de mayo del 2021). https://static.legis.pe/wp-content/uploads/2019/09/Convenio-sobre-la-Ciberdelincuencia-Legis.pe_.pdf

Calderón, L. (2021). *La punibilidad del comportamiento del mulero o phisher-mule en derecho penal español. Revista penal México – Nº 18.* (22 de octubre del 2021). https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/377/307

Cury, E. (2011). *Derecho Penal Parte General.* Santiago: Ediciones UC.

Decreto Nº 165, 20 de marzo de 2020 (México).

Devia, E. (2017). "*Delito informático: Estafa informática del artículo 248.2 del código penal". (Tesis doctoral).* Universidad de Sevilla, España.

Díaz, C. (2019). *"La aplicación de la ley Nº. 30096 -Ley de delitos informáticos respecto a su regulación en el derecho penal peruano" (Tesis de Grado).* Universidad César Vallejo, Perú.

Díaz, S. (2020). "*Desarrollo de sistema de análisis automático de phishing". (Tesis de Maestría).* Universidad Autónoma de Madrid, España.

Eguiguren, F. (2015). *El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú.* Lima: Themis Revista De Derecho.

Flores, C. (2017). *El phishing como comportamiento penalmente relevante.* Pontificia Universidad Católica de Valparaíso, Chile.

Flórez, I., & Díaz, L. (2017). "*Decisiones judiciales de suplantación de sitios web bancarios para capturar datos personales". (Tesis de Grado).* Universidad Libre, Colombia.

Ford, E. (2015). *El reto de la democracia digita. Hacia una ciudadanía interconectada.* Lima: Tarea Asociación Gráfica Educativa.

Frankel, S. (2015). International Copyright Problem and Durable Solutions, The. Vand. J. Ent. & Tech. L., 18, 39. http://www.law.columbia.edu/sites/default/files/microsites/kernochan/09-international-copyright-problem-durable-solutions.pdf

García, F. (2013). *Metodología de la investigación en las ciencias jurídicas y criminológicas, 4a. ed.* México: Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas CESCIJUC.

Gómez, M. (2006). *Introducción a la metodología de la investigación.* Argentina: Editorial Brujas.

Hernández, R., Fernández, C., & Baptista. (2014). *Metodología de la investigación (6ª ed.).* México: McGrwall Hill Education.

Herrera, L. (2018). "*Eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017". (Tesis de Grado).* Universidad de Huánuco, Perú.

Izcara, S. (2014). *Manual de investigación cualitativa.* México: Editorial Fontamara.

La ciberdelincuencia: ¿quién nos protege? (30 de abril del 2021) *Su regulación en Perú.* https://lpderecho.pe/la-ciberdelincuencia-quien-nos-protege/

Ley Nº 11.179. 25 de junio de 2008 (Argentina).

Ley Nº 19.223, 7 de junio de 1993 (Chile).

Ley Nº 1273. Normatividad sobre delitos informáticos. 05 de enero de 2009. (Colombia).

Ley Nº 30096. Delitos Informáticos. 22 de octubre de 2013. (Perú).

Ley Nº 30171. Modifica la Ley Nº 30096. Delitos Informáticos. 10 de marzo de 2014. (Perú).

Ley Orgánica 2/2019, 1 de marzo de 2019 (España).

López, E. (2007). *La investigación jurídica*. México: Porrúa.

López, M. (2014). "*Análisis jurídico del phishing como un delito informático encuadrado dentro del ámbito de las estafas". (Tesis de grado).* Universidad Mariano Gálvez, Guatemala.

Mengoa, M. (2021). "*Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú". (Tesis de grado).* Universidad César Vallejo, Perú.

Montaperto, J. (2018). "*Suplantación de Identidad: Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino". (Tesis de Grado).* Universidad Siglo 21, Argentina.

Montoya, F. (2017). *"Regulación expresa del delito informático de clonación de tarjetas - Sede DIVINDAT, 2017". (Tesis de Grado).* Universidad César Vallejo, Perú.

Morán, G., & Alvarado, D. (2010). *Métodos de investigación.* México: Pearson.

Novoa, E. (2005). *Curso de Derecho Penal Chileno Parte General.* Santiago: Editorial Jurídica de Chile.

Ortiz, J. (2013). *La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación.* Madrid: Fundación Alternativas.

Proyecto de Ley Nº 2661. 25 de febrero de 2008 (Estados unidos).

Rivero, L. (2017). Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano en el 2017. Universidad César Vallejo, Perú.

INCIBE (2016). Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario. Instituto Nacional De Ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Uterras, P. (2017). *"La necesidad de tipificar el delito de fraude informático en chile". (Tesis de Grado).* Universidad de Chile, Chile.

ANEXOS

ANEXO Nº 01: MATRIZ DE CATEGORIZACIÓN APRIORÍSTICA

MATRIZ DE CATEGORIZACIÓN						
TÍTULO INVESTIGATIVO	**PROBLEMA**	**PREGUNTAS DE INVESTIGACIÓN**	**OBJETIVO GENERAL**	**OBJETIVO ESPECÍFICO**	**CATEGORIAS**	**SUBCATEGORIAS**
EL PHISHING Y SU VULNERACIÓN A LA PROTECCIÓN DE DATOS PERSONALES EN LOS DELITOS INFORMÁTICOS	¿DE QUÉ MANERA EL PHISHING VULNERA LA PROTECCIÓN DE DATOS PERSONALES EN LOS DELITOS INFORMÁTICOS?	¿En qué consiste los alcances e impactos del phishing como apropiación de datos personales?	Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.	a) Explicar los alcances e impactos del phishing como apropiación de datos personales.	PHISHING	Naturaleza jurídica Definiciones teóricas Tipos y clasificación
		¿Cuál es la explicación de la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad?		b) Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad.		
		¿De qué manera se configuran los presupuestos de los delitos informáticos en el código penal peruano?		c) Analizar los presupuestos de los delitos informáticos en el código penal peruano.	DELITOS INFORMÁTICOS	Naturaleza jurídica Modalidades

ANEXO Nº 02: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: …….. **HORA:** ……..

LUGAR: ……..

ENTREVISTADOR: .....

ENTREVISTADO(A): .....

CARGO/PROFESIÓN: .....

INSTITUCIÓN: .....

INTRODUCCIÓN: La finalidad de la presente entrevista es determinar de qué manera el phishing vulnera la protección de datos personales en los delitos informáticos en el Perú. En tal sentido, el participante elegido ostenta amplia trayectoria en la materia, por lo que sus aportes serán de suma utilidad para la presente investigación.

Objetivo General:

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 1: (Solo Responde Profesional de Ingeniería de Sistemas)

Explicar los alcances e impactos del phishing como apropiación de datos personales

1. ¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?

……

……

……

2. ¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?

……

……

……

3. ¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?

……

……

……

Objetivo específico 2:

Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad

4. ¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?

……

……

……

5. ¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?

……

……

……

6. ¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?

……

……

……

Objetivo específico 3:

Analizar los presupuestos de los delitos informáticos en el código penal peruano.

7. ¿Considera que la vigente Ley Nº 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?

……

……

……

8. ¿Sería pertinente la creación de nuevos tipos penales? Explique

……

……

……

9. ¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?

……

……

……

_____

Nombre y firma del entrevistado

ANEXO Nº 03

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS JUECES

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del cuestionario/ guía de entrevista o ficha de recolección de datos, el mismo que le mostramos a continuación, indique de acuerdo a su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado pero debe ser modificado**
3	**Descriptor adecuado**

Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Apellidos y Nombres	Villanueva Sánchez Grover Eduardo
Grado Académico	Master of Business Administration – MBA Executive Doctor en Administración
Mención	Ingeniero de Sistemas Licenciado en Administración
Firma	

Trujillo, 10 de Setiembre del 2021

(Solo Responde Profesional de Ingeniería de Sistemas)

N°	Categorías / Ítems	Calificación Del Juez			Observación
	Categoría: phishing	1	2	3	
1	¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?			X	
2	¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?			X	
3	¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?			X	

P.D. Las preguntas me parecen pertinentes en relación a la categoría, sobre todo si se han considerado las suficientes para la investigación – responsabilidad del investigador, sin embargo, está claro que deberán incorporarse las diversas alternativas en cada una de ellas.

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS JUECES

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del cuestionario/ guía de entrevista o ficha de recolección de datos, el mismo que le mostramos a continuación, indique de acuerdo a su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado pero debe ser modificado**
3	**Descriptor adecuado**

Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Apellidos y Nombres	Salinas Ruiz Henry Eduardo
Grado Académico	Doctor
Mención	Gestión Pública y Gobernabilidad
Firma	

Trujillo, 13 de Agosto del 2021

Nº	Categorías / Ítems	Calificación Del Juez			Observación
	Categoría: Datos Personales	1	2	3	
4	¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?			X	
5	¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?			X	
6	¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?			X	

Nº	Categorías / Ítems	Calificación Del Juez			Observación
	Categoría: Delitos Informáticos	1	2	3	
7	¿Considera que la vigente Ley Nº 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?			X	
8	¿Sería pertinente la creación de nuevos tipos penales? Explique.			X	
9	¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?			X	

VALIDEZ DE TEST: JUICIO DE EXPERTOS

INSTRUCTIVO PARA LOS JUECES

Indicación: Señor especialista se le pide su colaboración para que luego de un riguroso análisis de los ítems del cuestionario/ guía de entrevista o ficha de recolección de datos, el mismo que le mostramos a continuación, indique de acuerdo a su criterio y su experiencia profesional el puntaje de acuerdo a si la pregunta permite capturar las variables de investigación del trabajo.

En la evaluación de cada ítem, utilice la siguiente escala:

RANGO	SIGNIFICADO
1	**Descriptor no adecuado y debe ser eliminado**
2	**Descriptor adecuado pero debe ser modificado**
3	**Descriptor adecuado**

Los rangos de la escala propuesta deben ser utilizados teniendo en consideración los siguientes criterios:

- Vocabulario adecuado al nivel académico de los entrevistados.
- Claridad en la redacción.
- Consistencia Lógica y Metodológica.

Apellidos y Nombres	Alcántara Ponce Leoncio Abel
Grado Académico	Maestría
Mención	Investigación y enseñanza Superior
Firma	CALL 7214

Trujillo, 30 de Junio del 2021

Nº	Categorías / Ítems	Calificación Del Juez			Observación
	Categoría: Datos Personales	1	2	3	
4	¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?			X	
5	¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?			X	
6	¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?			X	

Nº	Categorías / Ítems	Calificación Del Juez			Observación
	Categoría: Delitos Informáticos	1	2	3	
7	¿Considera que la vigente Ley Nº 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?			X	
8	¿Sería pertinente la creación de nuevos tipos penales? Explique.			X	
9	¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?			X	

ANEXO Nº 04

ANEXO Nº2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: 15-09-21 **HORA:** 11:30 a.m.

LUGAR: Trujillo

ENTREVISTADO(A): Becque Cesar T. Mimbela Veintimilla

CARGO/PROFESIÓN: ABOGADO

INSTITUCIÓN: ESTUDIO MIMBELA & ASOCIADOS

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 1: (Solo Responde Profesional de Ingeniería de Sistemas)

Explicar los alcances e impactos del phishing como apropiación de datos personales

1. ¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?

.....

.....

.....

.....

.....

2. ¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?

.....

.....

.....

.....

.....

3. ¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?

.....
.....
.....
.....
.....

Objetivo específico 2:

Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad

4. ¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?

.....
CASTIGANDO POR EL DELITO de Trafico ilicito de Datos, castigando a quien atente contra la intimidad, sirviendo como Consecuencia de la violacion a la intimidad.

5. ¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?

La normativa es eficaz, la desventaja es la falta de información por parte de los usuarios de internet que al no conocer la normativa no hacen sudenuncia a tiempo.
.....

6. ¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?

Pueden Ser sujetos a hurto, extorsión, y demas delitos que atenten contra la intimidad.
.....
.....

Objetivo específico 3:

Analizar los presupuestos de los delitos informáticos en el código penal peruano.

7. ¿Considera que la vigente Ley Nº 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?

La Ley tiene que sufrir modificacion y adaptarse a la realidad actual, pues cambio mucho la sociedad despues del Estado de emergencia.

8. ¿Sería pertinente la creación de nuevos tipos penales? Explique

Si, porque a evolucionado la utilización de medios electronicos, sobre todo en la administración publica.

9. ¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?

No, porque, este delito siempre es doloso, no hay culpa, siempre es doloso.

Muchas gracias por su valiosa opinión

Nombre y firma del entrevistado

Becque C. T. Mumbela Veintemilla
ABOGADO
CALL. 9423

UNIVERSIDAD CÉSAR VALLEJO

ANEXO N°2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: 22 set.2021 **HORA:** 09.30

LUGAR: Lima.

ENTREVISTADO(A): Dr.DAVID SAUL PAULETT HAUYON

CARGO/PROFESIÓN : DTP.ABOGADO

INSTITUCIÓN: UCV

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 2:

Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad

4. ¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?

El CP protege a la persona que son victimas del phishing mediante los delitos informáticos a fin de que no sean vulnerados su intimidad o privacity,seguro algunos no saben pero tienen la oportunidad de consultar a un abogado de esta protección

5. ¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?

Todos los países tienen buenas normas solo es que deben aplicarse y hacer valer sus derechos, en nuestro caso la norma es eficaz sin embargo algunos abogados creen que los delitos informáticos solo protegen sobre la máquina y no saben que lo que protegen es la intimidad de su contenido que se vulnera o rompe su clave para introducirse y viene

6. ¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?

Como idicamos en la pregunta anterior lo que se protege es su intimidad cuando se introducen rompiendo su clave,lo que suceda internamente en esa máquina nos conlleva a otros delitos es decir la máquina es el medio.

Objetivo específico 3:

Analizar los presupuestos de los delitos informáticos en el código penal peruano.

7. ¿Considera que la vigente Ley N° 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?

No es deficiente,sino hay que saber utilizarla y aplicarla que únicamente y exclusivamente es el medio para cometer otros injustos penales.

8. ¿Sería pertinente la creación de nuevos tipos penales? Explique

No necesariamente esta bien definido en esa norma penal cuando se comete este injusto penal lo que sucede es saber utilizarla y conectarla con otros delitos que se cometen que serían un concurso ideal de delitos

9. ¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?

En principio todo delito tiene autores y coautores son los hechos que van demostrar la participación de cada uno de los agentes, dado que toda violación a cualquier norma pena el órgano jurisdiccional debe identificar a estos agentes

UNIVERSIDAD CÉSAR VALLEJO

ANEXO N°2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: 22-09-2021 **HORA:** 4.00 pm.

LUGAR: Lima - Virtual.

ENTREVISTADO(A): Mag. Eliseo Wenzel Miranda.

CARGO/PROFESIÓN: Abogado – Docente Asesor

INSTITUCIÓN: Universidad Cesar Vallejo – Lima Norte.....

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 2:

Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad

4. ¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?

El Código Penal, de acuerdo a la tutela de derechos otorgados por el Estado, no detalla con precisión la protección ante el delito de phishing, dejando acción al conocimiento y diligencia del titular del bien.

5. ¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?

Como tal para el delito de phishing, no está taxativamente definido.

6. ¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?

La afectación es de carácter patrimonial definitivamente puesto que el autor material se apodera de los datos para conseguir un beneficio material. Los daños colaterales o consecuentes también pueden afectar a la intimidad,

Objetivo específico 3:

Analizar los presupuestos de los delitos informáticos en el código penal peruano.

7. ¿Considera que la vigente Ley N° 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?

Le falta mayor precisión, se hace necesario una nueva implementación normativa al respecto sobre todo es esta coyuntura actual donde este tipo de delitos se han incrementado.

8. ¿Sería pertinente la creación de nuevos tipos penales? Explique

Desde luego que es muy pertinente la creación de nuevos tipos penales considerando que la capacidad operativa de la ciber delincuencia se nutre de la tecnología, por tanto es necesario una nueva calificación típica y sus agravantes por la naturaleza misma del ilícito penal.

9. ¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?

Considero que si, definitivamente son delitos dolosos y sobre todo que se aprovechan de la confianza de la victima para ocasionar el daño.

UNIVERSIDAD CÉSAR VALLEJO

ANEXO N°2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÌA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: 29SET2021. **HORA:** 22.00.

LUGAR: ...LIMA.

ENTREVISTADO(A): MG. LUDWIN FIDEL PEÑA ALCA .....

CARGO/PROFESIÓN: DTC .....

INSTITUCIÓN: UCV-CAMPUS SAN JUAN DE LURIGANCHO .....

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 2:

Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad

4. ¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta el desconocimiento de las personas al ser víctimas del delito de phishing?

El Phishing es uno de los delitos cibernéticos más comunes en el país la practica radica en el envió de correos electrónicos para engañar a las personas y dirigirlos a páginas falsas que extraen información bancaria con la que los ladrones toman el dinero de las víctimas, esta conducta es precursora de delitos especialmente patrimoniales ya que permite obtener los datos de una cuenta bancaria (Loguin y password), tarjeta de créditos o sus datos personales obteniendo trasferencias no autorizadas, el desconocimiento y poco conocimiento de las personas relacionados a las funciones de los sistemas de cómputo permite que estos sujetos puedan engañar a los ciudadanos y mediante un ordenador puedan acceder a datos relacionado a su ámbito personal; en tal sentido el Código Penal en su Art. 154 protege el derecho a la intimidad el cual tiene una relevancia constitucional, sin embargo al emplear un equipo de cómputo para el acceso de datos estos se encontrarían inmersos en la Ley de Delitos Informáticos (Ley 30096) la cual protege la

interceptación de datos informáticos específicamente de datos personales o situaciones personales que atenten contra la intimidad.

5. ¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú? si existe una debida regulación en cuanto a los delitos informáticos en razón de que. Debido a su gran variedad y especialidad, la tarea de tipificación de los delitos informáticos resulta una labor muy complicada, por lo que se hace necesario delimitar con mucha precisión las características adecuadas de la criminalización de estas conductas y, por, sobre todo, el bien jurídico afectado como base de la sistematización. Como sabemos el derecho a la intimidad tiene una protección constitucional Art. 2do. Numeral 7 en el Perú, para proteger estos intereses se promulgo la Ley de Delitos Informáticos (Ley 30096), la misma que no se encuentra en un cuerpo normativo como es el código penal, si no en una Ley Especial en cuyo capitulo IV se sanciona los delitos contra la intimidad y el secreto de las comunicaciones, conformado por el Art. 6 (derogado por la Ley 30171) la cual modifica la Ley 30096 y el Art. 7 (interceptación de datos informáticos) en este caso, el Derecho Penal sanciona a quien intercepta de manera indebida información sensible en un sistema informático, que podría ser la identidad de sus miembros, referencias personales, números de cuentas bancarias, datos que en manos extrañas podrían causar graves daños económicos y morales, en líneas generales el delito de interceptación de datos informáticos busca evitar el uso abusivo de los medios informáticos, específicamente la divulgación y trasmisión de datos o situaciones personales que atenten contra la intimidad personal.

6. ¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?

Los datos personales e íntimos de las personas en manos extrañas podrían causar graves daños económicos y morales, específicamente la divulgación y trasmisión de datos o situaciones personales que atenten contra la intimidad personal.

Objetivo específico 3:

Analizar los presupuestos de los delitos informáticos en el código penal peruano.

7. ¿Considera que la vigente Ley Nº 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú? No es deficiente por los conceptos

expuestos líneas arriba (pregunta 5), lo que se necesita es un control en torno al acceso de los datos personales y la venta de los mismos por sujetos inescrupulosos.

8. ¿Sería pertinente la creación de nuevos tipos penales? Explique Como sabemos el Derecho Penal debe ser la última ratio, motivo por el cual no debe ser utilizado en todo proceso de criminalización, debiendo echar mano o crear otros medios de control social que tengan una relevancia menos gravosa y pueda controlar todo el tráfico de la información de datos relacionados a ordenadores informáticos.

9. ¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú? el phisher es la persona quien manipula o crea la página fraudulenta mediante el uso del ordenador con la finalidad de acceder a datos personales e íntimos de las personas que son engañadas en tal sentido es el autor directo y la gravosidad del hecho se debe tener en cuenta con relación al daño ocasionado teniendo en cuenta el sentido de la proporcionalidad de la pena.

Muchas gracias por su valiosa opinión

Nombre y firma del entrevistado

UNIVERSIDAD CÉSAR VALLEJO

ANEXO N°2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FEHCA: 10/10/21 **HORA:** 09:00 pm **LUGAR:** Trujillo

ENTREVISTADO(A): Dr. Julio Ivan Peña Quispe
CARGO/PROFESIÓN: Abogado
INSTITUCIÓN: Independiente

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 2:

Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad

4. ¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing? El código penal peruano en su art. 154 refiere la protección del derecho a la intimidad; sin embargo al emplear medios electrónicos el delito de phishing está inmerso en la ley de Delitos Informáticos, la cual protege información confidencial que vulnera la intimidad.

5. ¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú? En el art. 154 del código penal peruano se estipula el derecho a la intimidad personal o familiar, donde se advierte que quien viola dicho derecho valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de la libertad no menor de 2 años, lo cual es muy básico y no es más que un susurro amedrentamiento a una acción delictiva delicada dado que como todos sabemos una pena de no más de 2 años es una pena sin efectividad de cárcel o cumplimiento de la misma, por lo que no se protege en si en fin de cuentas el derecho a la libertad por la poca severidad del castigo impuesto.

6. ¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?

La persona sufre la violación de un derecho propio como el de la intimidad personal y familiar, lo cual muchas veces acaba en la comisión de otros delitos como la extorsión, la estafa, violación de derechos de autor, suplantación de identidad, etc.

Objetivo específico 3:

Analizar los presupuestos de los delitos informáticos en el código penal peruano.

7. ¿Considera que la vigente Ley N° 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?

Si es deficiente, dado que si así no fuera no se daría la Violación del secreto de las comunicaciones. Interceptación de comunicaciones personales de manera ilegal, utilización y modificación de los datos de carácter personal sin consentimiento, acceso ilegal a datos y sistemas informáticos; pero como vemos esto se da comúnmente en movimientos financieros y aun recolección de blancos empresariales a nivel nacional.

8. ¿Sería pertinente la creación de nuevos tipos penales? Explique

Sí, todo en el derechos es renovable y mejorable; y en cuanto a nuevos tipos penales sería bueno que esto abarque des una pena privativa de libertad más severa hasta la complicidad y actuación en banda o como organización criminal a quien actúen en conjunto aprovechando de sus conocimientos técnicos en la materia, inclusive el retiro o cese de algún estudio superior en la materia como consecuencia de su inequívoca utilización de ello en fines delictivos.

9. ¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú?

Así es, toda acción dolosa es un plus de consideración agravante, es menester que los delitos de phisher puedan formar parte ya los delitos informáticos y sus extensiones; dado que un phisher no es una persona ignorante en el tema sino muchas veces de personas técnicas o que usan implementos técnicos que se aprovechan de la ignorancia o desconocimiento de otros ciudadanos que de buena fe movidos por el uso de la tecnología caigan en este tipo de abusos y violación de derechos ya mencionados como la intimidad personal y familiar.

Dr. Julio Iván Peña Quispe
ABOGADO
CALI N° 612003

Nombre y firma del entrevistado

UNIVERSIDAD CÉSAR VALLEJO

ANEXO Nº2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: 21/09/2021 **HORA:** 10:45 pm

LUGAR: Virtual (Entrevista enviada vía Messenger)

ENTREVISTADO(A): Víctor M. Fernández Varas

CARGO/PROFESIÓN: Responsable de Mejora Continua / Ing. Sistemas

INSTITUCIÓN: Catering Manzanita Express SAC

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 1: (Solo Responde Profesional de Ingeniería de Sistemas)

Explicar los alcances e impactos del phishing como apropiación de datos personales

1. **¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?**

   El Phishing es uno de los grandes problemas que podemos encontrar en Internet hoy en día -y la primera técnica existente a través del tiempo conocida como parte de las técnicas de Ingeniería Social- utilizada por los cibercriminales para *engañar* a usuarios incautos mediante la *suplantación de identidad* (***estafa***) a través de cualquier medio electrónico o de telecomunicación, y lograr que estos les envíen *datos confidenciales* (información considerada como sensible) con la finalidad de *obtener un beneficio económico* de estos y a través de estos, ocasionando en los usuarios estafados desde el ***hurto*** (delito contra el patrimonio) hasta la ***utilización de sus cuentas y equipos*** (robo de identidad) para otras actividades delictivas que pueden ser de la misma índole o no.

2. **¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?**

   Si bien es cierto antes de la actual pandemia los bancos ya habían comenzado a implementar la plataforma virtual para casi todas las transacciones que sean referidas a dinero contable en cuentas propias, *los datos que tienen de todos sus clientes es una información de carácter sensible*, por lo que se debe de considerar 2 aspectos fundamentales. El primero es el referido a la *custodia de dicha información*, debiendo para ello implementar medidas de seguridad permanentes que resguarden dicha información; lo segundo es referida a la responsabilidad de la banca online, la cual debe de ser tomada como de *naturaleza casi objetiva*, derivada de la exigencia a la entidad titular del servicio de adoptar medidas de seguridad necesarias y renovables ante los distintos modos de fraude informático, de tal modo que, salvo que se acredite la negligencia grave por parte del usuario de la banca electrónica, la entidad financiera debe responder del reintegro de los importes obtenidos de forma fraudulenta.

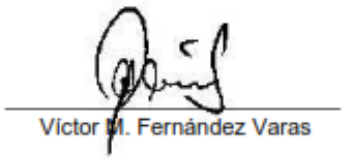
3. **¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?**

   A la entidad le corresponde capacitar y evaluar de manera constante al personal que tiene a su cargo referidos al área de Tecnologías de la Información acerca de las amenazas existentes y conforme vayan apareciendo referidas al fraude informático de este tipo, para así acreditar que las operaciones ordenadas sí fueron auténticas y que no estuvo afectada por un fallo técnico o por otra deficiencia como, por ejemplo, por un ataque informático de naturaleza fraudulenta al sistema bancario que hubiera permitido el acceso a las cuentas de sus clientes y disponer ilícitamente, de las mismas ordenando operaciones en detrimento de estos. Así mismo, iniciar de manera conjunta con otros bancos por medio de las asociaciones existentes, o de manera individual, campañas mediáticas que informen y ayuden a implementar una cultura de prevención en sus clientes acerca de los cuidados que deben de tener con respecto al Phishing.

   Por el lado de los clientes, debemos de tener la obligación de llevar a cabo las recomendaciones brindadas por las entidades bancarias, así como tener el cuidado de asegurarse por diferentes medios que es el banco el que realiza las comunicaciones que recibe y de no realizar transacciones fuera de los canales conocidos y permitidos por la institución financiera.

UNIVERSIDAD CÉSAR VALLEJO

Muchas gracias por su valiosa opinión



Víctor M. Fernández Varas

UNIVERSIDAD CÉSAR VALLEJO

ANEXO N°2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: 28/09/2021..... **HORA:** 06:03 pm.....

LUGAR: Trujillo.

ENTREVISTADO(A): Javier Jacinto Jáuregui

CARGO/PROFESIÓN: Ingeniero de Sistemas .....

INSTITUCIÓN: Asesor Externo de nuevas tecnologías.....

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 1: (Solo Responde Profesional de Ingeniería de Sistemas)

Explicar los alcances e impactos del phishing como apropiación de datos personales

1. ¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?

El único peligro y fatal para la víctima es la violación a su información confidencial, el cual tiene valor constitutivo de su privacidad.

.....

.....

2. ¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?

En toda medida, las financieras deben garantizar y ser responsables de la seguridad de la información de todos sus clientes. Actualmente, se cuenta con la tecnología para rastrear las operaciones o transacciones.

.....

3. ¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?

Deben emplear, todos los mecanismos básicos pero seguros que garanticen la confiabilidad, la integridad y la disponibilidad de la información al realizar las operaciones, en los trabajos de: Autenticación, Detectivos y Correctivos.

.....

.....

Muchas gracias por su valiosa opinión

Ing. R. Javier Jacinto Jáuregui

Nombre y firma del entrevistado

UNIVERSIDAD CÉSAR VALLEJO

ANEXO N°2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: ……26/09/2021…… ..... **HORA:** 10:00 PM

LUGAR: La Esperanza

ENTREVISTADO(A): ELMER GUARNIZ GUARNIZ

CARGO/PROFESIÓN: SOPORTE TECNICO Y TI

INSTITUCIÓN: ISTP SAN LUIS

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 1: (Solo Responde Profesional de Ingeniería de Sistemas)

Explicar los alcances e impactos del phishing como apropiación de datos personales

1. ¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?

Como se sabe, el Phising o suplantación de identidad es un fenómeno que expone datos personales a personas ajenas, entonces la persona o entidad afectada corre un alto riesgo al hacerse mal uso de ellos.

Adquisición de servicios, algunos bienes o realización de transacciones no autorizadas que pueden terminar incluso en el robo de dinero en las cuentas personales o de la empresa.

2. ¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?

Los bancos y cualquier empresa que nos provee de algún servicio donde se almacenan nuestros datos debe tomar conciencia de que son los responsables de esos datos y contratar especialistas que permitan asegurar que no sean difundidos por un ataque

informático y sobre todo, prevenir el caso de convenios con terceros para la adquisición de nuevos productos a través de terceros.

3. ¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?

Como mencionamos, fundamentalmente contratar servicios especializados para evitar el ataque informático y por ende el robo de la información personal del usuario, un buen data center por ejemplo. Además, se podría pensar en evaluar la manera de como se implementa la cartera de clientes, es decir la manera de buscar nuevos clientes, se tiene algunas referencias por ejemplo que se recurre al mercado negro para la adquisición de bases de datos de usuarios del mercado negro para este tipo de prácticas, cosa que según se tiene entendido, esta penado, pero lamentablemente en nuestro país no se cumple la ley, de hacerlo tendríamos mejores sistemas y los datos del usuario a buen recaudo.

Muchas gracias por su valiosa opinión

Ing. Elmer Guarniz Guarniz

Nombre y firma del entrevistado

UNIVERSIDAD CÉSAR VALLEJO

ANEXO N°2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: 24/09/2021 **HORA:** 15:30

LUGAR: .....

ENTREVISTADO(A): José Francisco Bobadilla Castro

CARGO/PROFESIÓN: Experto en Aplicaciones / Ing. de Computación y Sistemas

INSTITUCIÓN: Universidad Privada del Norte

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 1: (Solo Responde Profesional de Ingeniería de Sistemas)

Explicar los alcances e impactos del phishing como apropiación de datos personales

1. ¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?

Los ciberdelincuentes pueden utilizar la información personal robada mediante phising para distintos fines como: suplantación de identidad, robo de dinero en bancos, espionaje y utilización de las cuentas robadas para fines delictivos.

2. ¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?

Cada vez que se brindan datos personales a una empresa, como un banco, se encuentran en la obligación de informar a sus clientes la finalidad con la que será usada esta información, de esta forma se está asegurando la protección de la misma respecto a fines distintos a los acordados.

3. ¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?

El phising es una estafa lanzada a una persona. En ese sentido, los bancos sólo pueden optar por hacer campañas de concientización para informar a sus clientes sobre el adecuado uso de sus plataformas y funcionamiento de sus medios de comunicación. Por el lado de los clientes, informarse sobre el tema, tomar tests y reforzar la seguridad de su ordenador con un antivirus, sistema operativo y navegadores actualizados.

Muchas gracias por su valiosa opinión

Ing. José Francisco Bobadilla Castro

Nombre y firma del entrevistado

UNIVERSIDAD CESAR VALLEJO

ANEXO N°2: INSTRUMENTO DE RECOLECCION DE DATOS.

GUÍA DE ENTREVISTA.

Título: "El phishing y su vulneración a la protección de datos personales en los delitos informáticos."

FECHA: [illegible]

HORA: .....

LUGAR: Trujillo

ENTREVISTADO(A): Ing. Walter Alexander Julián Sánchez

CARGO/PROFESIÓN: Sub Gerente de Tecnología de la Información y Comunicaciones

INSTITUCIÓN: Municipalidad Distrital de El Porvenir

Objetivo General

Determinar si el phishing vulnera la protección de datos personales en los delitos informáticos.

Objetivo específico 1: (Solo Responde Profesional de Ingeniería de Sistemas)

Explicar los alcances e impactos del phishing como apropiación de datos personales

1. ¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?

Usurpación de identidad informática, utilizan data personal y credencial de cuentas para ser usada delincuencia maliciosa

2. ¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?

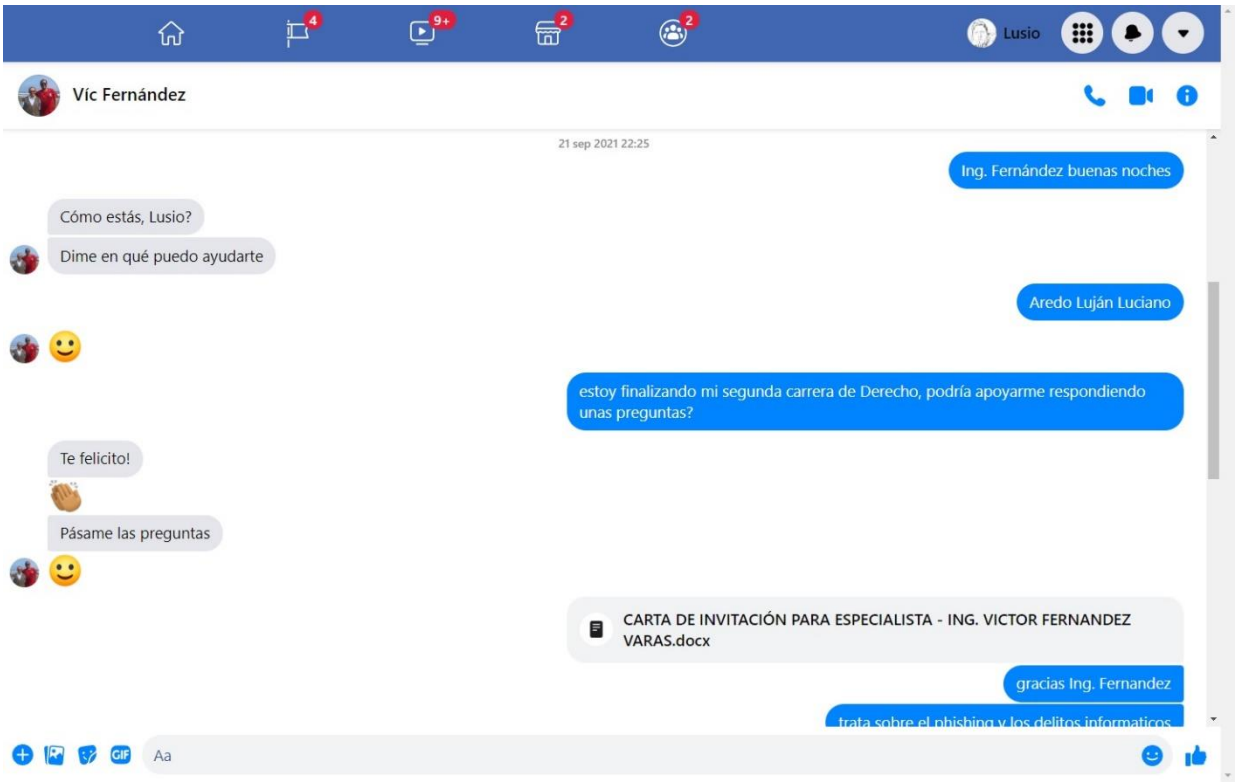
No 6 100% y solo registra la transacción; ahora si desean protegar su tarjeta piden una comisión a pago mensual y para ahora así no apoyan al 100%

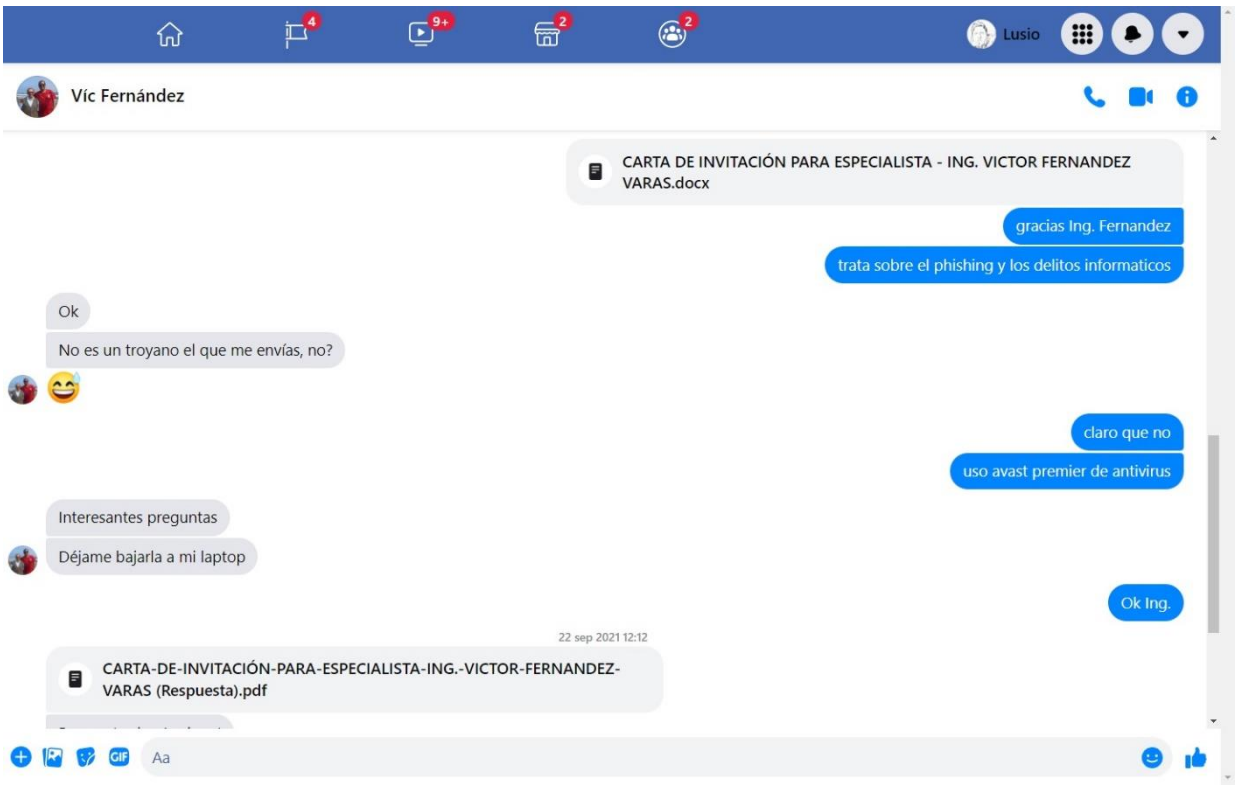
UNIVERSIDAD CÉSAR VALLEJO

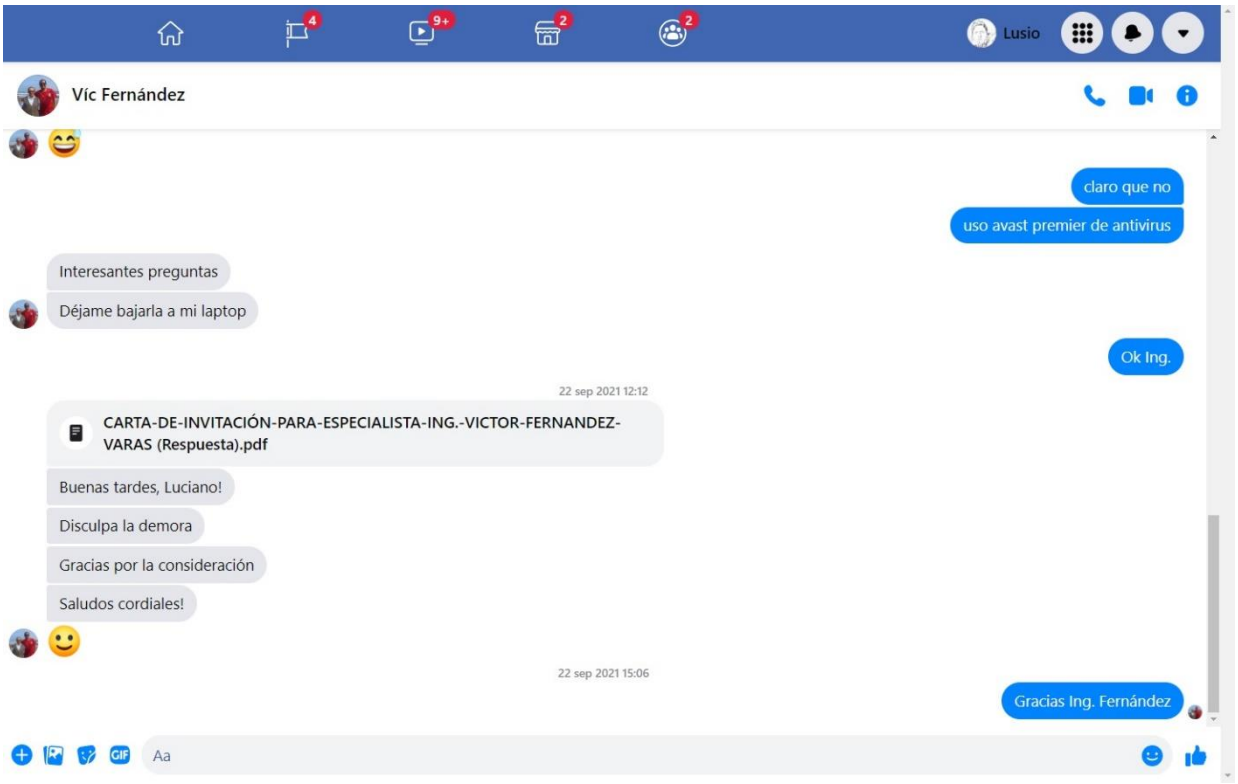
3. ¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?

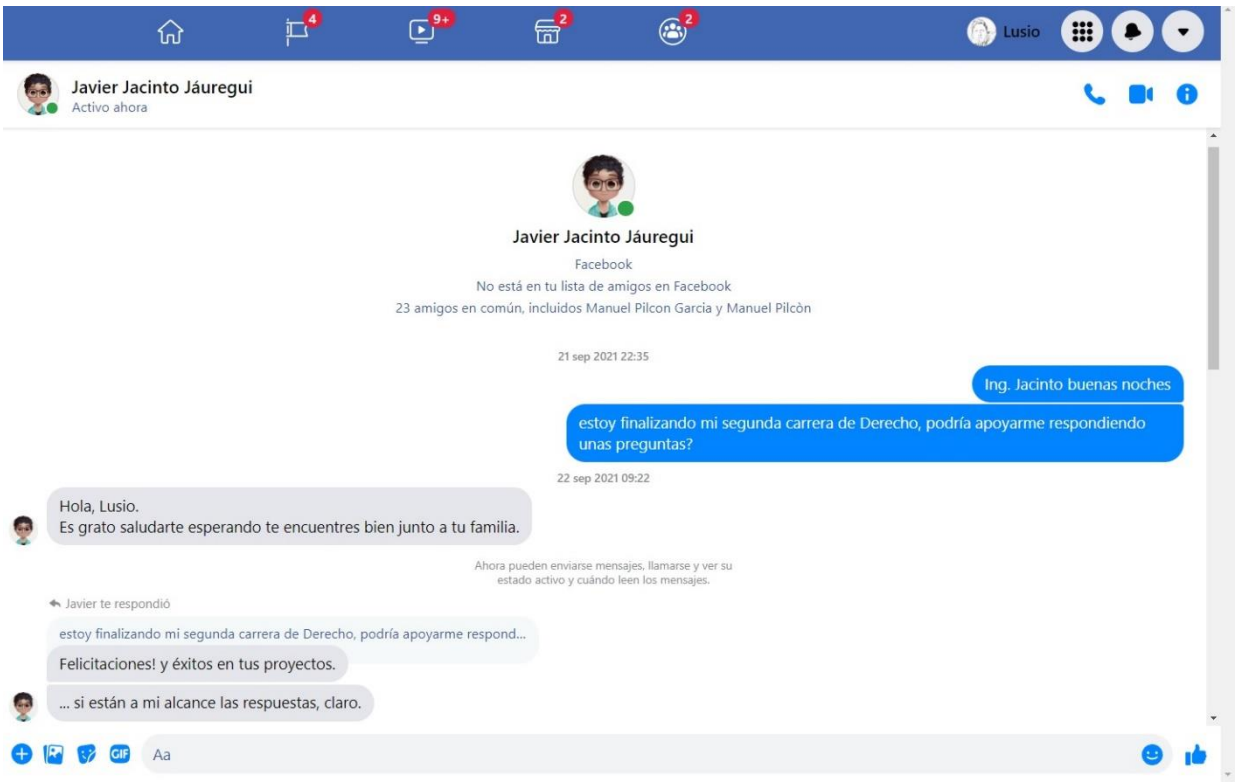
los mecanismos de seguridad del Banco es constante pero no ayuda al 100%.

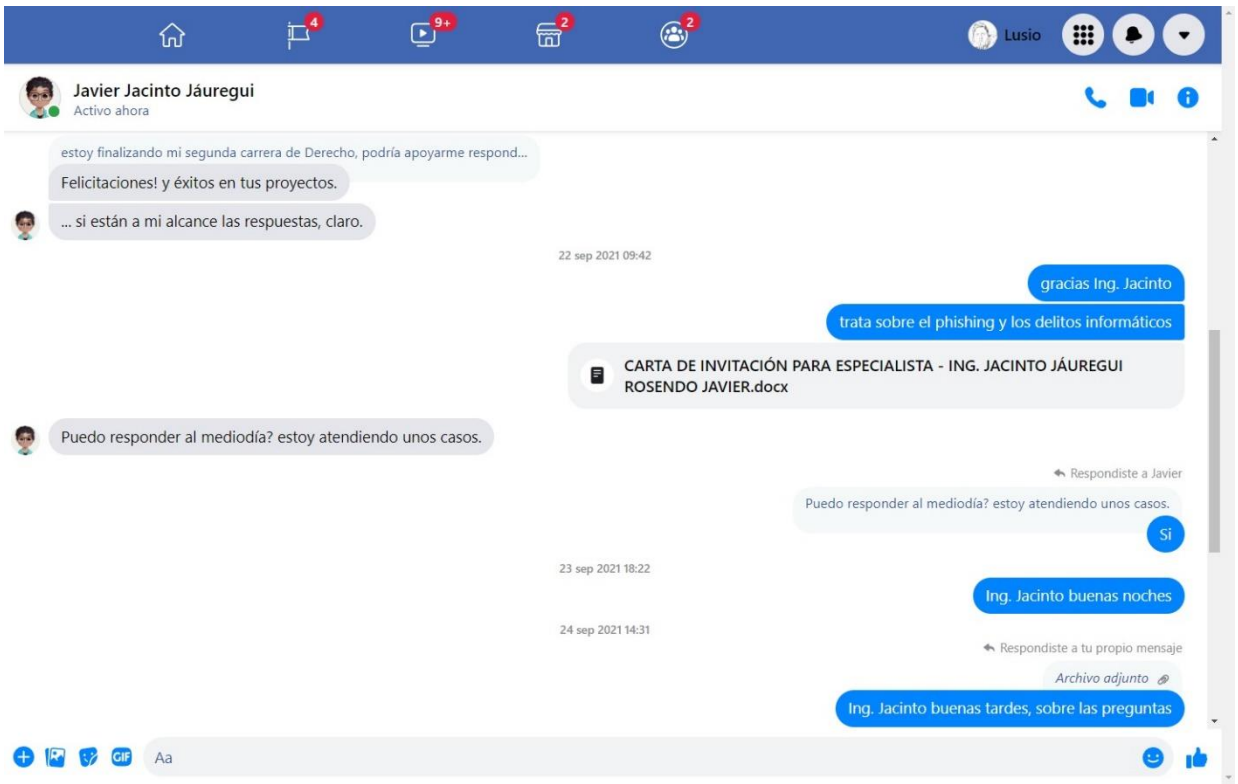
los clientes son la clave de protegor sus credenciales utilizando una red privada y utilizar su propio Equipo informatico en doble o mayor seguridad posible.

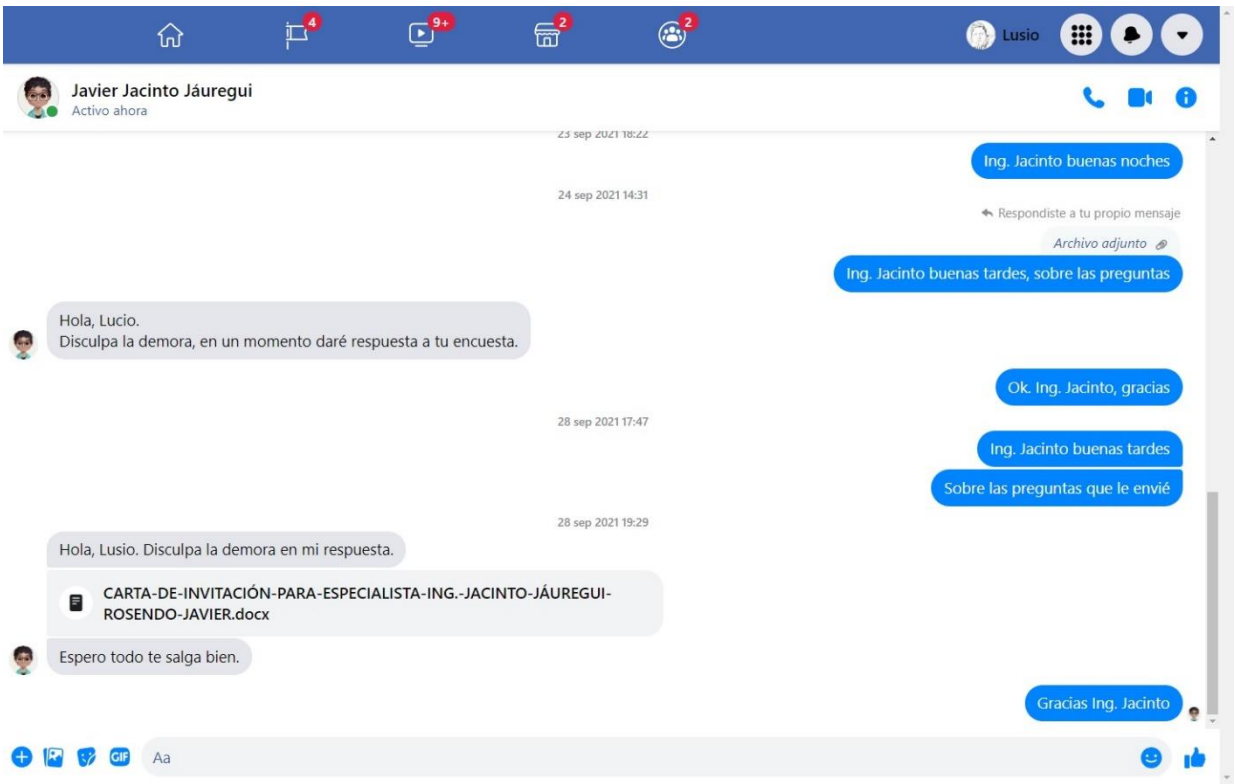

Lusio
Víc Fernández
21 sep 2021 22:25
Ing. Fernández buenas noches
Cómo estás, Lusio?
Dime en qué puedo ayudarte
Aredo Luján Luciano
estoy finalizando mi segunda carrera de Derecho, podría apoyarme respondiendo unas preguntas?
Te felicito!
Pásame las preguntas
CARTA DE INVITACIÓN PARA ESPECIALISTA - ING. VICTOR FERNANDEZ VARAS.docx
gracias Ing. Fernandez
trata sobre el phishing y los delitos informaticos
Aa

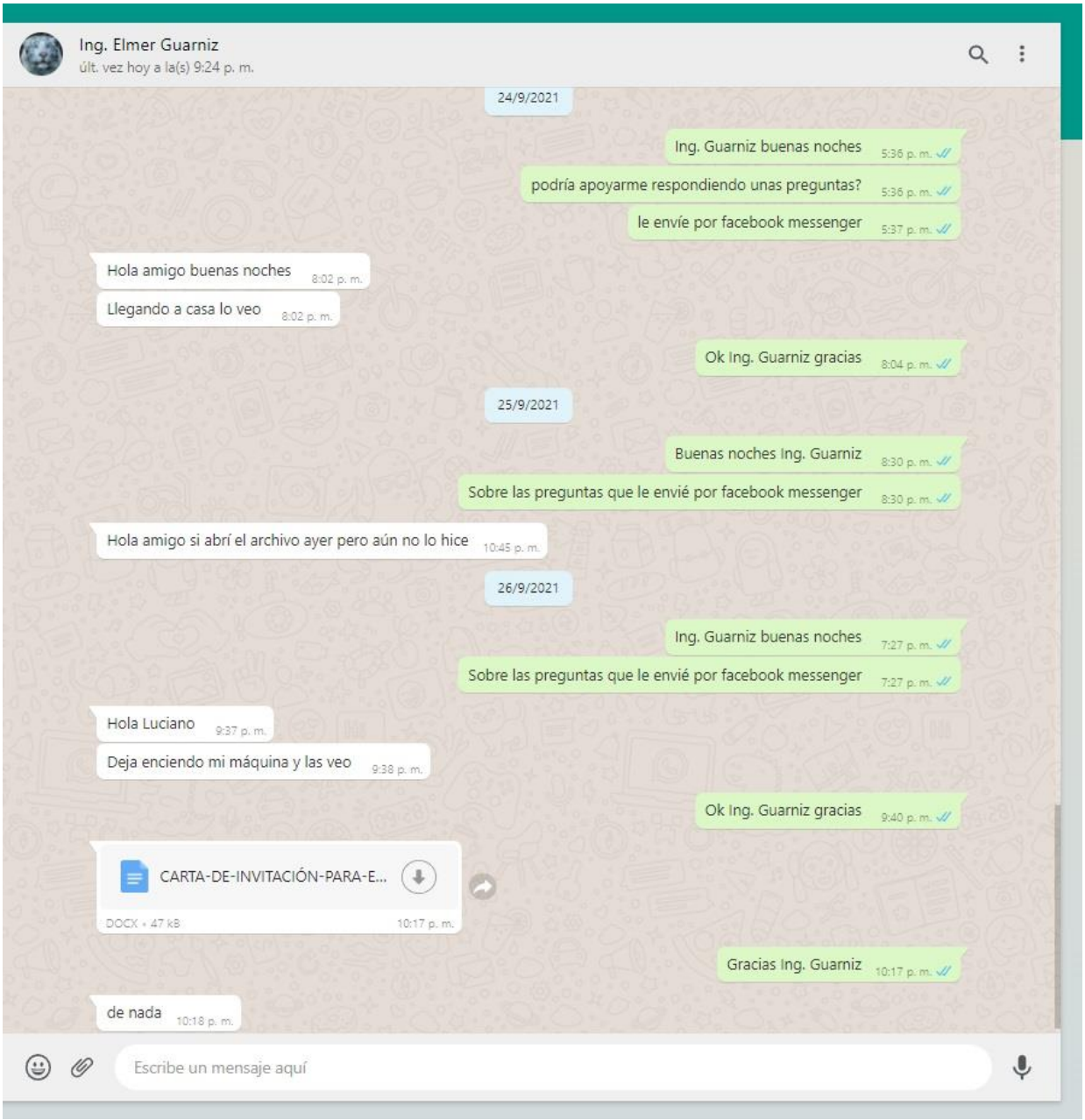

Lusio
Víc Fernández
CARTA DE INVITACIÓN PARA ESPECIALISTA - ING. VICTOR FERNANDEZ VARAS.docx
gracias Ing. Fernandez
trata sobre el phishing y los delitos informaticos
Ok
No es un troyano el que me envías, no?
claro que no
uso avast premier de antivirus
Interesantes preguntas
Déjame bajarla a mi laptop
Ok Ing.
22 sep 2021 12:12
CARTA-DE-INVITACIÓN-PARA-ESPECIALISTA-ING.-VICTOR-FERNANDEZ-VARAS (Respuesta).pdf
Aa

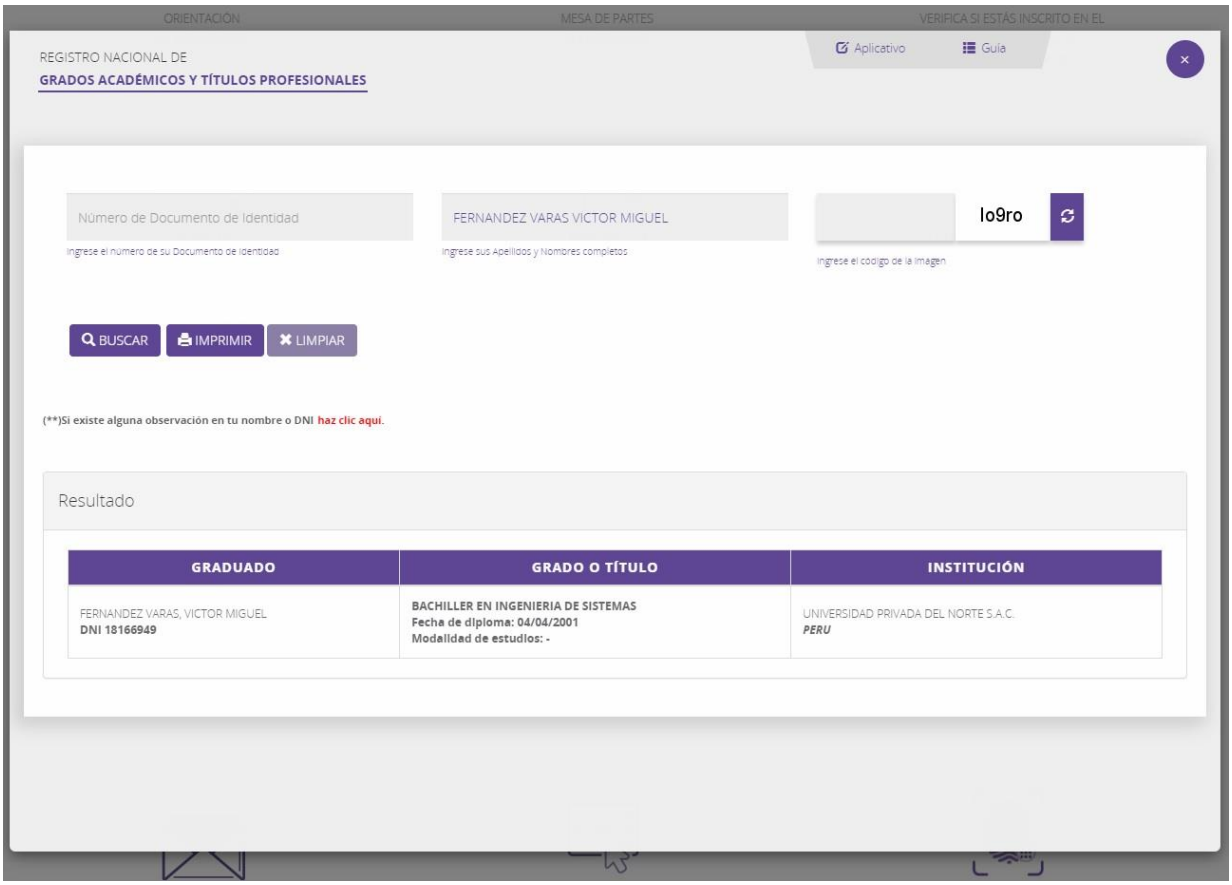

Lusio
Víc Fernández
claro que no
uso avast premier de antivirus
Interesantes preguntas
Déjame bajarla a mi laptop
Ok Ing.
22 sep 2021 12:12
CARTA-DE-INVITACIÓN-PARA-ESPECIALISTA-ING.-VICTOR-FERNANDEZ-VARAS (Respuesta).pdf
Buenas tardes, Luciano!
Disculpa la demora
Gracias por la consideración
Saludos cordiales!
22 sep 2021 15:06
Gracias Ing. Fernández
Aa

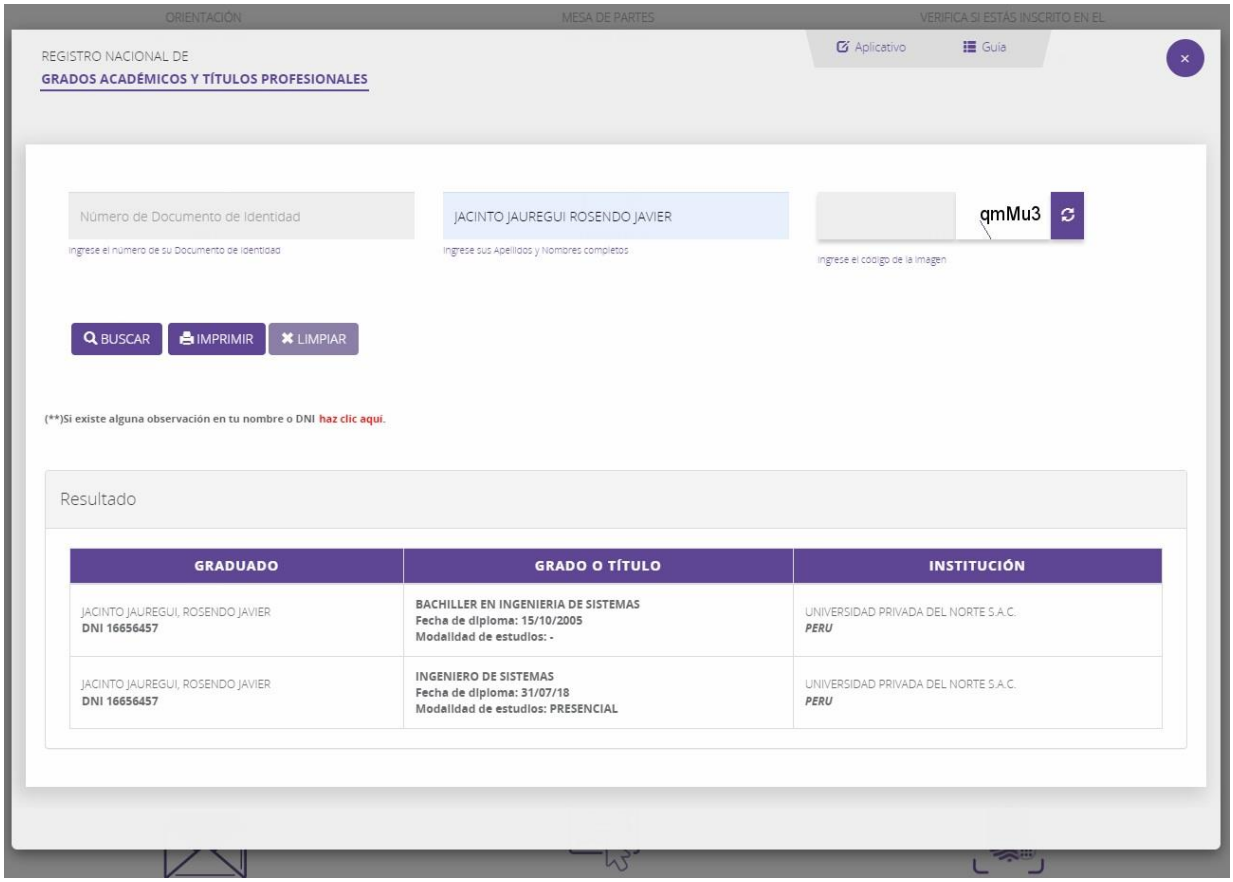

Lusio
Javier Jacinto Jáuregui
Activo ahora
Javier Jacinto Jáuregui
Facebook
No está en tu lista de amigos en Facebook
23 amigos en común, incluidos Manuel Pilcon Garcia y Manuel Pilcòn
21 sep 2021 22:35
Ing. Jacinto buenas noches
estoy finalizando mi segunda carrera de Derecho, podría apoyarme respondiendo unas preguntas?
22 sep 2021 09:22
Hola, Lusio.
Es grato saludarte esperando te encuentres bien junto a tu familia.
Ahora pueden enviarse mensajes, llamarse y ver su estado activo y cuándo leen los mensajes.
Javier te respondió
estoy finalizando mi segunda carrera de Derecho, podría apoyarme respond...
Felicitaciones! y éxitos en tus proyectos.
... si están a mi alcance las respuestas, claro.
Aa

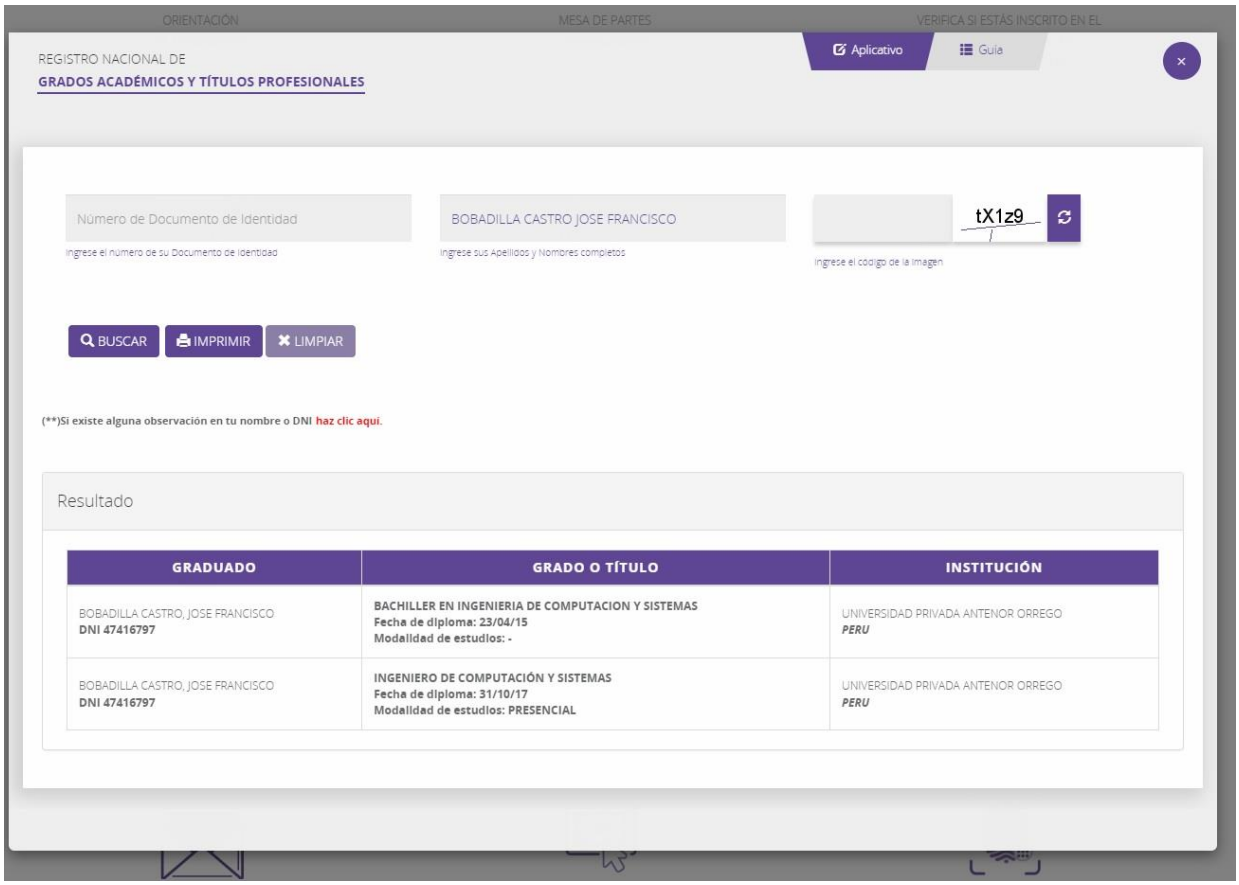

Lusio
Javier Jacinto Jáuregui
Activo ahora
estoy finalizando mi segunda carrera de Derecho, podría apoyarme respond...
Felicitaciones! y éxitos en tus proyectos.
... si están a mi alcance las respuestas, claro.
22 sep 2021 09:42
gracias Ing. Jacinto
trata sobre el phishing y los delitos informáticos
CARTA DE INVITACIÓN PARA ESPECIALISTA - ING. JACINTO JÁUREGUI ROSENDO JAVIER.docx
Puedo responder al mediodía? estoy atendiendo unos casos.
Respondiste a Javier
Puedo responder al mediodía? estoy atendiendo unos casos.
Si
23 sep 2021 18:22
Ing. Jacinto buenas noches
24 sep 2021 14:31
Respondiste a tu propio mensaje
Archivo adjunto
Ing. Jacinto buenas tardes, sobre las preguntas
Aa

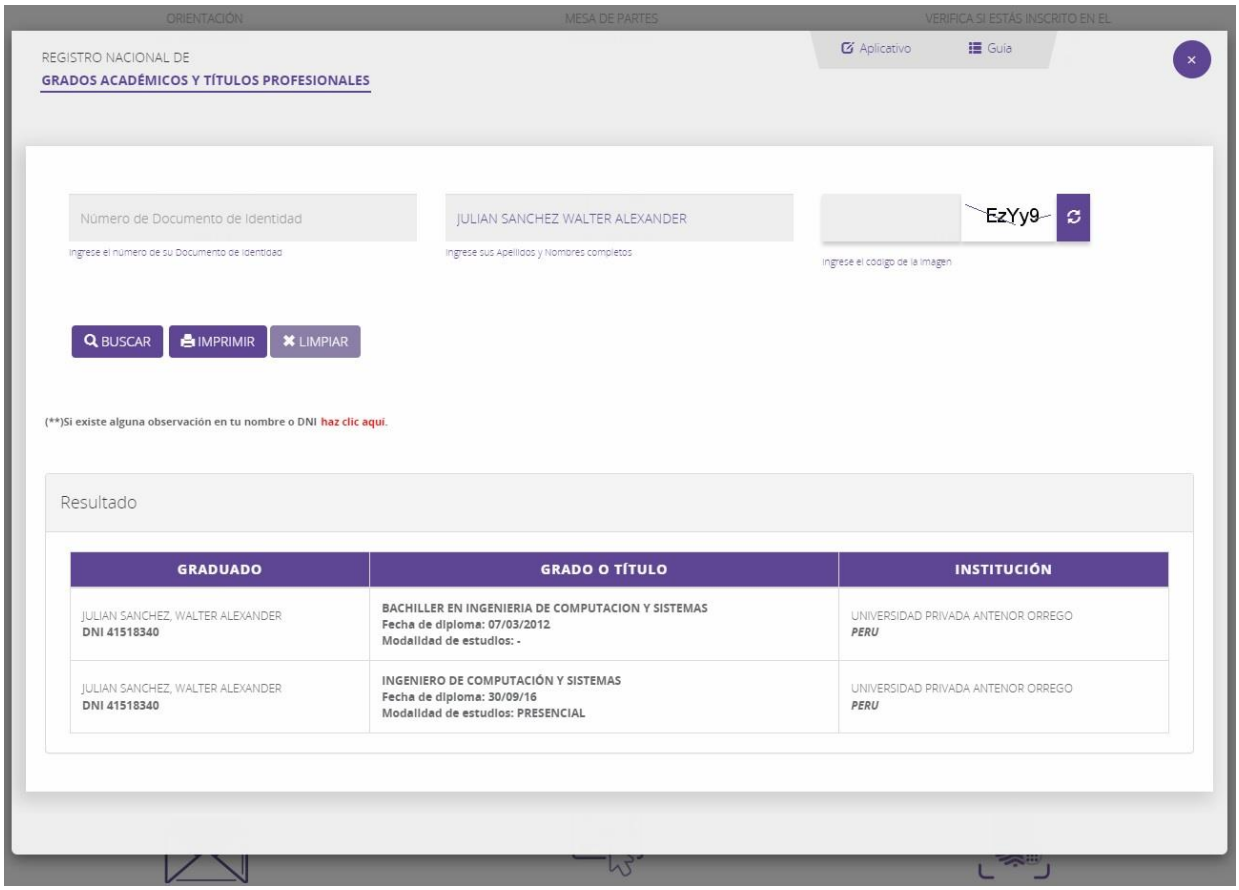

Lusio
Javier Jacinto Jáuregui
Activo ahora
23 sep 2021 18:22
Ing. Jacinto buenas noches
24 sep 2021 14:31
Respondiste a tu propio mensaje
Archivo adjunto
Ing. Jacinto buenas tardes, sobre las preguntas
Hola, Lucio.
Disculpa la demora, en un momento daré respuesta a tu encuesta.
Ok. Ing. Jacinto, gracias
28 sep 2021 17:47
Ing. Jacinto buenas tardes
Sobre las preguntas que le envié
28 sep 2021 19:29
Hola, Lusio. Disculpa la demora en mi respuesta.
CARTA-DE-INVITACIÓN-PARA-ESPECIALISTA-ING.-JACINTO-JÁUREGUI-ROSENDO-JAVIER.docx
Espero todo te salga bien.
Gracias Ing. Jacinto
Aa


Ing. Elmer Guarniz
últ. vez hoy a la(s) 9:24 p. m.
24/9/2021
Ing. Guarniz buenas noches 5:36 p. m.
podría apoyarme respondiendo unas preguntas? 5:36 p. m.
le envíe por facebook messenger 5:37 p. m.
Hola amigo buenas noches 8:02 p. m.
Llegando a casa lo veo 8:02 p. m.
Ok Ing. Guarniz gracias 8:04 p. m.
25/9/2021
Buenas noches Ing. Guarniz 8:30 p. m.
Sobre las preguntas que le envié por facebook messenger 8:30 p. m.
Hola amigo si abrí el archivo ayer pero aún no lo hice 10:45 p. m.
26/9/2021
Ing. Guarniz buenas noches 7:27 p. m.
Sobre las preguntas que le envié por facebook messenger 7:27 p. m.
Hola Luciano 9:37 p. m.
Deja enciendo mi máquina y las veo 9:38 p. m.
Ok Ing. Guarniz gracias 9:40 p. m.
CARTA-DE-INVITACIÓN-PARA-E...
DOCX • 47 kB 10:17 p. m.
Gracias Ing. Guarniz 10:17 p. m.
de nada 10:18 p. m.
Escribe un mensaje aquí


ORIENTACIÓN
MESA DE PARTES
VERIFICA SI ESTÁS INSCRITO EN EL
Aplicativo
Guía
REGISTRO NACIONAL DE
GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES
Número de Documento de Identidad
Ingrese el número de su Documento de Identidad
FERNANDEZ VARAS VICTOR MIGUEL
Ingrese sus Apellidos y Nombres completos
lo9ro
Ingrese el código de la imagen
BUSCAR
IMPRIMIR
LIMPIAR
(**)Si existe alguna observación en tu nombre o DNI haz clic aquí.
Resultado
GRADUADO
GRADO O TÍTULO
INSTITUCIÓN
FERNANDEZ VARAS, VICTOR MIGUEL
DNI 18166949
BACHILLER EN INGENIERIA DE SISTEMAS
Fecha de diploma: 04/04/2001
Modalidad de estudios: -
UNIVERSIDAD PRIVADA DEL NORTE S.A.C.
PERU


ORIENTACIÓN
MESA DE PARTES
VERIFICA SI ESTÁS INSCRITO EN EL
Aplicativo
Guía
REGISTRO NACIONAL DE
GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES
Número de Documento de Identidad
Ingrese el número de su Documento de Identidad
JACINTO JAUREGUI ROSENDO JAVIER
Ingrese sus Apellidos y Nombres completos
qmMu3
Ingrese el código de la imagen
BUSCAR
IMPRIMIR
LIMPIAR
(**)Si existe alguna observación en tu nombre o DNI haz clic aquí.
Resultado
GRADUADO
GRADO O TÍTULO
INSTITUCIÓN
JACINTO JAUREGUI, ROSENDO JAVIER
DNI 16656457
BACHILLER EN INGENIERIA DE SISTEMAS
Fecha de diploma: 15/10/2005
Modalidad de estudios: -
UNIVERSIDAD PRIVADA DEL NORTE S.A.C.
PERU
JACINTO JAUREGUI, ROSENDO JAVIER
DNI 16656457
INGENIERO DE SISTEMAS
Fecha de diploma: 31/07/18
Modalidad de estudios: PRESENCIAL
UNIVERSIDAD PRIVADA DEL NORTE S.A.C.
PERU


ORIENTACIÓN
MESA DE PARTES
VERIFICA SI ESTÁS INSCRITO EN EL
REGISTRO NACIONAL DE
GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES
Aplicativo
Guía
Número de Documento de Identidad
Ingrese el número de su Documento de Identidad
BOBADILLA CASTRO JOSE FRANCISCO
Ingrese sus Apellidos y Nombres completos
tX1z9
Ingrese el código de la imagen
BUSCAR
IMPRIMIR
LIMPIAR
(**)Si existe alguna observación en tu nombre o DNI haz clic aquí.
Resultado
GRADUADO
GRADO O TÍTULO
INSTITUCIÓN
BOBADILLA CASTRO, JOSE FRANCISCO
DNI 47416797
BACHILLER EN INGENIERIA DE COMPUTACION Y SISTEMAS
Fecha de diploma: 23/04/15
Modalidad de estudios: -
UNIVERSIDAD PRIVADA ANTENOR ORREGO
PERU
BOBADILLA CASTRO, JOSE FRANCISCO
DNI 47416797
INGENIERO DE COMPUTACIÓN Y SISTEMAS
Fecha de diploma: 31/10/17
Modalidad de estudios: PRESENCIAL
UNIVERSIDAD PRIVADA ANTENOR ORREGO
PERU


ORIENTACIÓN
MESA DE PARTES
VERIFICA SI ESTÁS INSCRITO EN EL
Aplicativo
Guía
REGISTRO NACIONAL DE
GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES
Número de Documento de Identidad
Ingrese el número de su Documento de Identidad
JULIAN SANCHEZ WALTER ALEXANDER
Ingrese sus Apellidos y Nombres completos
EzYy9
Ingrese el codigo de la imagen
BUSCAR
IMPRIMIR
LIMPIAR
(**)Si existe alguna observación en tu nombre o DNI haz clic aquí.
Resultado
GRADUADO
GRADO O TÍTULO
INSTITUCIÓN
JULIAN SANCHEZ, WALTER ALEXANDER
DNI 41518340
BACHILLER EN INGENIERIA DE COMPUTACION Y SISTEMAS
Fecha de diploma: 07/03/2012
Modalidad de estudios: -
UNIVERSIDAD PRIVADA ANTENOR ORREGO
PERU
JULIAN SANCHEZ, WALTER ALEXANDER
DNI 41518340
INGENIERO DE COMPUTACIÓN Y SISTEMAS
Fecha de diploma: 30/09/16
Modalidad de estudios: PRESENCIAL
UNIVERSIDAD PRIVADA ANTENOR ORREGO
PERU

ANEXO Nº 05

OBJETIVO ESPECIFICO Nº 1: Explicar los alcances e impactos del phishing como apropiación de datos personales

TABLA 1: Respuesta de los especialistas respecto de la pregunta 1 de la entrevista

¿Cuáles son los peligros a los que se exponen los datos personales en cuanto al delito de phishing?	
Entrevistado	**Respuesta**
Ingeniero 1	El Phishing es uno de los grandes problemas que podemos encontrar en Internet hoy en día -y la primera técnica existente a través del tiempo conocida como parte de las técnicas de Ingeniería Social- utilizada por los cibercriminales para engañar a usuarios incautos mediante la suplantación de identidad (estafa) a través de cualquier medio electrónico o de telecomunicación, y lograr que estos les envíen datos confidenciales (información considerada como sensible) con la finalidad de obtener un beneficio económico de estos y a través de estos, ocasionando en los usuarios estafados desde el hurto (delito contra el patrimonio) hasta la utilización de sus cuentas y equipos (robo de identidad) para otras actividades delictivas que pueden ser de la misma índole o no.
Ingeniero 2	El único peligro y fatal para la víctima es la violación a su información confidencial, el cual tiene valor constitutivo de su privacidad.
Ingeniero 3	Los ciberdelincuentes pueden utilizar la información personal robada mediante phising para distintos fines como: suplantación de identidad, robo de dinero en bancos, espionaje y utilización de las cuentas robadas para fines delictivos.
Ingeniero 4	Usurpación de identidad informática, utilizan datos personales y credenciales de cuentas para ser usados de forma maliciosa.
Ingeniero 5	Como se sabe, el Phising o suplantación de identidad es un fenómeno que expone datos personales a personas ajenas, entonces la persona o entidad afectada corre un alto riesgo al hacerse mal uso de ellos. Adquisición de servicios, algunos bienes o realización de transacciones no autorizadas que pueden terminar incluso en el robo de dinero en las cuentas personales o de la empresa.

ANEXO Nº 06

TABLA 2: Respuesta de los especialistas respecto de la pregunta 2 de la entrevista

¿En qué medida, los bancos son responsables de proteger los datos personales de sus clientes frente al delito de phishing?	
Entrevistado	**Respuesta**
Ingeniero 1	Si bien es cierto antes de la actual pandemia los bancos ya habían comenzado a implementar la plataforma virtual para casi todas las transacciones que sean referidas a dinero contable en cuentas propias, los datos que tienen de todos sus clientes es una información de carácter sensible, por lo que se debe de considerar 2 aspectos fundamentales. El primero es el referido a la custodia de dicha información, debiendo para ello implementar medidas de seguridad permanentes que resguarden dicha información; lo segundo es referida a la responsabilidad de la banca online, la cual debe de ser tomada como de naturaleza casi objetiva, derivada de la exigencia a la entidad titular del servicio de adoptar medidas de seguridad necesarias y renovables ante los distintos modos de fraude informático, de tal modo que, salvo que se acredite la negligencia grave por parte del usuario de la banca electrónica, la entidad financiera debe responder del reintegro de los importes obtenidos de forma fraudulenta.
Ingeniero 2	En toda medida, las financieras deben garantizar y ser responsables de la seguridad de la información de todos sus clientes. Actualmente, se cuenta con la tecnología para rastrear las operaciones o transacciones.
Ingeniero 3	Cada vez que se brindan datos personales a una empresa, como un banco, se encuentran en la obligación de informar a sus clientes la finalidad con la que será usada esta información, de esta forma se está asegurando la protección de la misma respecto a fines distintos a los acordados.
Ingeniero 4	No es 100%, solo registran las transacciones; ahora si desean proteger sus tarjetas piden una comisión o pago mensual, pero aun así no apoyan al 100%
Ingeniero 5	Los bancos y cualquier empresa que nos provee de algún servicio donde se almacenan nuestros datos debe tomar conciencia de que son los responsables de esos datos y contratar especialistas que permitan asegurar que no sean difundidos por un ataque informático y sobre todo, prevenir el caso de convenios con terceros para la adquisición de nuevos productos a través de terceros.

ANEXO Nº 07

TABLA 3: Respuesta de los especialistas respecto de la pregunta 3 de la entrevista

¿Qué mecanismos de seguridad deberían emplear las entidades bancarias y los clientes frente al delito de phishing?	
Entrevistado	**Respuesta**
Ingeniero 1	A la entidad le corresponde capacitar y evaluar de manera constante al personal que tiene a su cargo referidos al área de Tecnologías de la Información acerca de las amenazas existentes y conforme vayan apareciendo referidas al fraude informático de este tipo, para así acreditar que las operaciones ordenadas sí fueron auténticas y que no estuvo afectada por un fallo técnico o por otra deficiencia como, por ejemplo, por un ataque informático de naturaleza fraudulenta al sistema bancario que hubiera permitido el acceso a las cuentas de sus clientes y disponer ilícitamente, de las mismas ordenando operaciones en detrimento de estos. Así mismo, iniciar de manera conjunta con otros bancos por medio de las asociaciones existentes, o de manera individual, campañas mediáticas que informen y ayuden a implementar una cultura de prevención en sus clientes acerca de los cuidados que deben de tener con respecto al Phishing. Por el lado de los clientes, debemos de tener la obligación de llevar a cabo las recomendaciones brindadas por las entidades bancarias, así como tener el cuidado de asegurarse por diferentes medios que es el banco el que realiza las comunicaciones que recibe y de no realizar transacciones fuera de los canales conocidos y permitidos por la institución financiera.
Ingeniero 2	Deben emplear, todos los mecanismos básicos pero seguros que garanticen la confiabilidad, la integridad y la disponibilidad de la información al realizar las operaciones, en los trabajos de: Autenticación, Detectivos y Correctivos.
Ingeniero 3	El phising es una estafa lanzada a una persona. En ese sentido, los bancos sólo pueden optar por hacer campañas de concientización para informar a sus clientes sobre el adecuado uso de sus plataformas y funcionamiento de sus medios de comunicación. Por el lado de los clientes, informarse sobre el tema, tomar tests y reforzar la seguridad de su ordenador con un antivirus, sistema operativo y navegadores actualizados.
Ingeniero 4	Los mecanismos de seguridad del banco son constantes, pero no ayudan al 100%. Los clientes son la clave de proteger sus credenciales, utilizando una red privada y utilizar su propio equipo informático posible o mayor seguridad posible.
Ingeniero 5	Como mencionamos, fundamentalmente contratar servicios especializados para evitar el ataque informático y por ende el robo de la información personal del usuario, un buen data center, por ejemplo. Además, se podría pensar en evaluar la manera de cómo se implementa la cartera de clientes, es decir la manera de buscar nuevos clientes, se tiene algunas referencias por ejemplo que se recurre al mercado negro para la adquisición de bases de datos de usuarios del mercado negro para este tipo de prácticas, cosa que según se tiene entendido, está penado, pero lamentablemente en nuestro país no se cumple la ley, de hacerlo tendríamos mejores sistemas y los datos del usuario a buen recaudo.

ANEXO Nº 08

OBJETIVO ESPECIFICO Nº 2: Explicar la importancia de cautelar los datos personales como garantía de protección del derecho a la intimidad

TABLA 4: Respuesta de los especialistas respecto de la pregunta 4 de la entrevista

¿De qué manera se protege el derecho a la intimidad en el código penal teniendo en cuenta la ignorancia de las personas al ser víctimas del delito de phishing?	
Entrevistado	**Respuesta**
Abogado 1	Castigado por el delito de tráfico ilícito de datos, castigando a quien atente contra la intimidad, sirviendo como consecuencia de la violación a la intimidad
Abogado 2	El código penal peruano en su art. 154 refiere la protección del derecho a la intimidad; sin embargo, al emplear medios electrónicos el delito de phishing está inmerso en la ley de Delitos Informáticos, la cual protege información confidencial que vulnera la intimidad.
Abogado 3	El CP protege a la persona que son víctimas del phishing mediante los delitos informáticos a fin de que no sean vulnerados su intimidad o privacidad, y seguro algunos no saben, pero tienen la oportunidad de consultar a un abogado de esta protección
Abogado 4	El Código Penal, de acuerdo con la tutela de derechos otorgados por el Estado, no detalla con precisión la protección ante el delito de phishing, dejando acción al conocimiento y diligencia del titular del bien.
Abogado 5	El Phishing es uno de los delitos cibernéticos más comunes en el país la practica radica en el envió de correos electrónicos para engañar a las personas y dirigirlos a páginas falsas que extraen información bancaria con la que los ladrones toman el dinero de las víctimas, esta conducta es precursora de delitos especialmente patrimoniales ya que permite obtener los datos de una cuenta bancaria (Login y password), tarjeta de créditos o sus datos personales obteniendo trasferencias no autorizadas, el desconocimiento y poco conocimiento de las personas relacionados a las funciones de los sistemas de cómputo permite que estos sujetos puedan engañar a los ciudadanos y mediante un ordenador puedan acceder a datos relacionado a su ámbito personal; en tal sentido el Código Penal en su Art. 154 protege el derecho a la intimidad el cual tiene una relevancia constitucional, sin embargo al emplear un equipo de cómputo para el acceso de datos estos se encontrarían inmersos en la Ley de Delitos Informáticos (Ley Nº 30096) la cual protege la interceptación de datos informáticos específicamente de datos personales o situaciones personales que atenten contra la intimidad.

ANEXO Nº 09

TABLA 5: Respuesta de los especialistas respecto de la pregunta 5 de la entrevista

¿Considera que existe una regulación normativa eficaz de la protección del derecho a la intimidad en el código penal en los delitos informáticos en el Perú?	
Entrevistado	**Respuesta**
Abogado 1	La normativa es eficaz, la desventaja es la falta de información por parte de los usuarios de internet que al no conocer la normativa no hacen su denuncia a tiempo
Abogado 2	En el art. 154 del código penal peruano se estipula el derecho a la intimidad personal o familiar, donde se advierte que quien viola dicho derecho valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de la libertad no menor de 2 años, lo cual es muy básico y no es más que un susurro amedrentamiento a una acción delictiva delicada dado que como todos sabemos una pena de no más de 2 años es una pena sin efectividad de cárcel o cumplimiento de la misma, por lo que no se protege en si en fin de cuentas el derecho a la libertad por la poca severidad del castigo impuesto.
Abogado 3	Todos los países tienen buenas normas solo es que deben aplicarse y hacer valer sus derechos, en nuestro caso la norma es eficaz sin embargo algunos abogados creen que los delitos informáticos solo protegen sobre la máquina y no saben que lo que protegen es la intimidad de su contenido que se vulnera o rompe su clave para introducirse y viene
Abogado 4	Como tal para el delito de phishing, no está taxativamente definido.
Abogado 5	Debido a su gran variedad y especialidad, la tarea de tipificación de los delitos informáticos resulta una labor muy complicada, por lo que se hace necesario delimitar con mucha precisión las características adecuadas de la criminalización de estas conductas y, por, sobre todo, el bien jurídico afectado como base de la sistematización. Como sabemos el derecho a la intimidad tiene una protección constitucional Art. 2do. Numeral 7 en el Perú, para proteger estos intereses se promulgo la Ley de Delitos Informáticos (Ley 30096), la misma que no se encuentra en un cuerpo normativo como es el código penal, si no en una Ley Especial en cuyo capitulo IV se sanciona los delitos contra la intimidad y el secreto de las comunicaciones, conformado por el Art. 6 (derogado por la Ley 30171) la cual modifica la Ley 30096 y el Art. 7 (interceptación de datos informáticos) en este caso, el Derecho Penal sanciona a quien intercepta de manera indebida información sensible en un sistema informático, que podría ser la identidad de sus miembros, referencias personales, números de cuentas bancarias, datos que en manos extrañas podrían causar graves daños económicos y morales, en líneas generales el delito de interceptación de datos informáticos busca evitar el uso abusivo de los medios informáticos, específicamente la divulgación y trasmisión de datos o situaciones personales que atenten contra la intimidad personal.

ANEXO Nº 10

TABLA 6: Respuesta de los especialistas respecto de la pregunta 6 de la entrevista

¿De qué forma se ve afectado la persona al acceder a sus datos personales en los delitos informáticos en el Perú?	
Entrevistado	**Respuesta**
Abogado 1	Pueden ser sujetos a hurto, extorsión, y demás delitos que atenten contra la intimidad
Abogado 2	La persona sufre la violación de un derecho propio como el de la intimidad personal y familiar, lo cual muchas veces acaba en la comisión de otros delitos como la extorsión, la estafa, violación de derechos de autor, suplantación de identidad, etc.
Abogado 3	Como indicamos en la pregunta anterior lo que se protege es su intimidad cuando se introducen rompiendo su clave, lo que suceda internamente en esa máquina nos conlleva a otros delitos es decir la máquina es el medio.
Abogado 4	La afectación es de carácter patrimonial definitivamente puesto que el autor material se apodera de los datos para conseguir un beneficio material. Los daños colaterales o consecuentes también pueden afectar a la intimidad
Abogado 5	Los datos personales e íntimos de las personas en manos extrañas podrían causar graves daños económicos y morales, específicamente la divulgación y trasmisión de datos o situaciones personales que atenten contra la intimidad personal.

ANEXO Nº 11

OBJETIVO ESPECIFICO Nº 3: Analizar los presupuestos de los delitos informáticos en el código penal peruano

TABLA 7: Respuesta de los especialistas respecto de la pregunta 7 de la entrevista

¿Considera que la vigente Ley Nº 30096 – Ley de Delitos Informáticos en aplicación del Derecho Penal es deficiente en el Perú?	
Entrevistado	**Respuesta**
Abogado 1	La ley tiene que sufrir modificación y adaptarse a la realidad actual, pues cambió mucho la sociedad después del Estado de emergencia
Abogado 2	Si es deficiente, dado que si así no fuera no se daría la Violación del secreto de las comunicaciones. Interceptación de comunicaciones personales de manera ilegal, utilización y modificación de los datos de carácter personal sin consentimiento, acceso ilegal a datos y sistemas informáticos; pero como vemos esto se da comúnmente en movimientos financieros y aun recolección de blancos empresariales a nivel nacional.
Abogado 3	No es deficiente, sino hay que saber utilizarla y aplicarla que única y exclusivamente es el medio para cometer otros injustos penales.
Abogado 4	Le falta mayor precisión, se hace necesario una nueva implementación normativa al respecto sobre todo en esta coyuntura actual donde este tipo de delitos se han incrementado.
Abogado 5	No es deficiente por los conceptos expuestos líneas arriba (pregunta 5), lo que se necesita es un control en torno al acceso de los datos personales y la venta de los mismos por sujetos inescrupulosos.

ANEXO Nº 12

TABLA 8: Respuesta de los especialistas respecto de la pregunta 8 de la entrevista

¿Sería pertinente la creación de nuevos tipos penales? Explique	
Entrevistado	**Respuesta**
Abogado 1	Si, porque ha evolucionado la utilización de medios electrónicos, sobre todo en la administración publica
Abogado 2	Sí, todo en el derecho es renovable y mejorable; y en cuanto a nuevos tipos penales sería bueno que esto abarque des una pena privativa de libertad más severa hasta la complicidad y actuación en banda o como organización criminal a quien actúen en conjunto aprovechando de sus conocimientos técnicos en la materia, inclusive el retiro o cese de algún estudio superior en la materia como consecuencia de su inequívoca utilización de ello en fines delictivos.
Abogado 3	No necesariamente, está bien definido en la norma penal. Cuando se comete este injusto penal lo que sucede es saber utilizarla y conectarla con otros delitos que se cometen, que serían un concurso ideal de delitos
Abogado 4	Desde luego que es muy pertinente la creación de nuevos tipos penales considerando que la capacidad operativa de la ciber delincuencia se nutre de la tecnología, por tanto, es necesaria una nueva calificación típica y sus agravantes por la naturaleza misma del ilícito penal.
Abogado 5	Como sabemos el Derecho Penal debe ser la última ratio, motivo por el cual no debe ser utilizado en todo proceso de criminalización, debiendo echar mano o crear otros medios de control social que tengan una relevancia menos gravosa y pueda controlar todo el tráfico de la información de datos relacionados a ordenadores informáticos.

ANEXO Nº 13

TABLA 9: Respuesta de los especialistas respecto de la pregunta 9 de la entrevista

¿Considera usted que si el phisher ha actuado de manera dolosa podría considerarse como agravante y de esta forma ser coautor en los delitos informáticos en el Perú	
Entrevistado	**Respuesta**
Abogado 1	No, porque este delito siempre es doloso, no hay culpa, siempre es doloso.
Abogado 2	Así es, toda acción dolosa es un plus de consideración agravante, es menester que los delitos de phisher puedan formar parte ya los delitos informáticos y sus extensiones; dado que un phisher no es una persona ignorante en el tema sino muchas veces de personas técnicas o que usan implementos técnicos que se aprovechan de la ignorancia o desconocimiento de otros ciudadanos que de buena fe movidos por el uso de la tecnología caigan en este tipo de abusos y violación de derechos ya mencionados como la intimidad personal y familiar.
Abogado 3	En principio todo delito tiene autores y coautores son los hechos que van a demostrar la participación de cada uno de los agentes, dado que toda violación a cualquier norma penal, el órgano jurisdiccional debe identificar a estos agentes.
Abogado 4	Considero que sí, definitivamente son delitos dolosos y sobre todo que se aprovechan de la confianza de la víctima para ocasionar el daño.
Abogado 5	El phisher es la persona quien manipula o crea la página fraudulenta mediante el uso del ordenador con la finalidad de acceder a datos personales e íntimos de las personas que son engañadas en tal sentido es el autor directo y la gravosidad del hecho se debe tener en cuenta con relación al daño ocasionado, teniendo en cuenta el sentido de la proporcionalidad de la pena.

ANEXO Nº 14

PROYECTO DE LEY: LEY QUE REGULA SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES

El Colegio de Abogados de La Libertad, debidamente representado por su Decano **Víctor Daniel Coronel Salaverry**, en estricto cumplimiento de lo dispuesto en el artículo 107º de la Constitución Política del Perú y de los artículos 75º y 76º del Reglamento del Congreso de la república presenta el siguiente proyecto de Ley:

I.- EXPOSICIÓN DE MOTIVOS

Según el artículo 17º, inciso 1, del Convenio Sobre La Ciberdelincuencia (Convenio de Budapest), ratificada por Estado peruano el 10 de marzo de 2019 establece que Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Que, hoy en día el phishing es el método de fraude online mayormente empleado, el proceder del término phishing, está basado en la llamada ingeniería social. Dicha práctica se basa en la manipulación de las personas mediante técnicas psicológicas o habilidades adquiridas, propias de la naturaleza humana. En el phishing, se envían mensajes ingeniosamente redactados solicitando información delicada, por medio del correo electrónico, llamadas telefónicas, vía sms, etc.

Que, el delito de phishing consiste en “Conducta delictiva diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños”.

Este proyecto de ley es necesario, debido al aumento de delitos informáticos, requerido en gran parte por la propagación de la pandemia Covid-19, lo que ha propiciado el incremento de las compras electrónicas, resulta de vital interés conocer cómo protegernos.

II.- EFECTO DE LA VIGENCIA DE LA NORMA QUE SE PROPONE SOBRE LA LEGISLACIÓN NACIONAL.

La presente iniciativa legislativa complementa la Ley 30096 - Ley de Delitos Informáticos.

III. ANÁLISIS COSTO - BENEFICIO DE LA FUTURA NORMA LEGAL

El impacto de la presente iniciativa legislativa resulta favorable en la medida en que, sin irrogar costo alguno al erario nacional, se fortalecerá la reglamentación de los delitos informáticos.

IV. FORMULA LEGAL

LEY QUE REGULA SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES

Artículo 1.- El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que de dicha conducta resulte algún perjuicio, material o moral y que la conducta no constituya delito sancionado con pena más grave.

Artículo 2.- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que de dicha conducta resulte algún perjuicio, material o moral y que la conducta no constituya delito sancionado con pena más grave.

Artículo 3.- La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Disposiciones finales

Primera.- En el plazo máximo de 180 días calendario se expedirá el Reglamento de la presente ley.

TRUJILLO, 29 de noviembre del 2021

LUCIANO ANTONIO AREDO LUJÁN

DNI 70493396