ESTUDIOS DE POSGRADO UNIVERSIDAD EAN

SEMINARIO DE INVESTIGACIÓN

AUTORES

MARIA FERNANDA MORA ZAMBRANO

Gerencia de procesos de calidad e innovación

NICHOLL STEFHANY QUINTERO OVALLE

Gerencia de procesos de calidad e innovación

JUAN DANIEL ALMONACID LOPEZ

Gerencia de proyectos

LIZETH KATHERIN MONROY MACIAS

Gerencia de proyectos

TUTOR

PABLO CESAR OCAMPO

BOGOTA D,C

MAYO 2022

Tabla de contenido

TABLA DE FIGURAS

LISTA DE TABLAS

Resumen

En la actualidad, a causa de los grandes avances tecnológicos que surgen, el sector financiero se ha visto impactado negativamente respecto a la seguridad informática conocida como *Phishing,* presentando perdidas no solo para los clientes, sino incluso, para las entidades financieras. En el presente documento se podrán evidenciar las técnicas más comunes que suelen usar los delincuentes cibernéticos para engañar las personas y poder generar dichos ataques; lo que se pretende con esta información recopilada es prevenir y/o evitar ataques que pretendan realizar y a su vez brindarles un poco de conocimiento sobre estos engaños para que antes de dar cualquier dato personal se aseguren de no estar siendo víctimas de *Phishing.*

Todo esto basados en la teoría de Ben D. Sawyer y Peter A. Hancock, quienes hablan de la existencia de una correlación directa entre la frecuencia de los mensajes de correo maliciosos y la identificación exitosa del usuario. En su teoría, estos investigadores se basaron en el "efecto de prevalencia" que es conocido en la psicología que expone la probabilidad de que una persona omita o no detecte una señal que indique una señal poco común confundiéndola con alguna situación que puede ocurrir normalmente.

Dicho esto, lo más conveniente fue realizar la investigación mediante una metodología cuantitativa, donde mediante encuestas a funcionarios bancarios se pretendía llegar a las experiencias de ciberataque que presentan muchos ciudadanos colombianos. Los resultados arrojados hacen llegar a la conclusión de que la mejor manera de brindar una solución a esta población vulnerable por ataques es la implementación del uso de inteligencia artificial y Machine learning ya que esto garantizaría la seguridad de datos ya que este tiene como fin el

saber con exactitud si la persona que está ingresando a la plataforma en efecto es el titular original del producto financiero.

Palabras clave: phishing, ciberseguridad, vulnerabilidad, GoPhish.

1. Planteamiento del Problema

Constantemente, debido a la expansión del internet como una herramienta indispensable y necesaria en la actualidad, y la adopción de sus facilidades tanto en ámbitos empresariales, académicos, personales y en general en la vida cotidiana de la humanidad, se han presentado múltiples maneras de robo por medio de suplantación de identidades a través de todo tipo de medios electrónicos. Esta metodología utiliza correos electrónicos de spam llamativos haciendo alusión a rifas y eventos falsos e incluso en ámbitos empresariales, enlaces referentes a relaciones con posibles clientes o información en general del mercado.

La suplantación de identidad es definida como “la apropiación indebida de otra identidad para actuar en su nombre; los objetivos del suplantador pueden ser múltiples, desde hacer una broma pesada, dañar la reputación o el peor escenario, realizar ciberataques desde la cuenta aprovechando la confianza que se genera en otras personas” (Conoldo, 2021, pág. 1).

Una metodología utilizada para ello es el *phishing*; el cual se basa en el robo de información por medio de plataformas de internet.

Leguizamón define el *phishing* como “el proceso por el cual una persona es contactada por email o por teléfono por alguien que simula ser una institución legítima para obtener datos privados, tales como información bancaria, contraseñas, datos personales, etc.; luego esta

información obtenida de forma fraudulenta es utilizada para acceder a las cuentas personales de las víctimas y causar pérdidas económicas o suplantación de identidad" (Leguizamon, 2015)

Existen a dos formas de *phishing*, una de ellas se basa en el engaño al que se somete al usuario, haciendo creer que su interlocutor es prestador de servicio en específico o a una entidad gubernamental confiable, la otra tiene que ver con la utilización de mecanismos puramente técnicos, a través de los cuales se logra el robo de la información de identificación y autenticación del usuario, sin que de ningún modo intervenga la voluntad inducida a error de éste.

Teniendo en cuenta la contextualización anterior, se hace evidente el problema que constituye el hecho de caer en páginas ilegales que de manera fraudulenta atacan al usuario de manera casi imperceptible para cometer robos y fraudes que atentan contra la seguridad de la información y de las transacciones online.

La tecnología ha evolucionado de manera significativa en los últimos años siendo uno de los pilares fundamentales para el crecimiento y la expansión del mercado y de la sociedad, brindando de este modo acceso ilimitado a todo tipo de información, mejorando los esquemas de prestación de servicios y contribuyendo a la interconexión y facilidad en la socialización y comunicación de las personas desde cualquier parte del mundo, incluso transacciones digitales para la obtención de productos y servicios sin necesidad de presencialidad.

Sin embargo, este desarrollo tecnológico no está blindado de las amenazas que rodean la integridad y confidencialidad de datos personales, pues a medida que los diferentes tipos de mercados giran en torno al desarrollo tecnológico, enfocados en la inclusión y participación activa en la era digital, se generan nuevas técnicas de fraudes, bien sea ataques masivos por

correos electrónicos, páginas web clonadas para la obtención de números de cuentas, tarjetas de créditos y demás metodologías atentan con la seguridad de la información.

Según Caballero & Cilleros (2020) argumentan que la Transformación digital está empujando a las empresas y a los profesionales a cambiar radicalmente su manera de pensar y trabajar. En un mundo donde tanto el 7 Cloud como los procesos de desarrollo Agile están a la orden del día, la seguridad tradicional debe transformarse para afrontar los nuevos retos y los constantes ataques y amenazas. Dicha transformación ha alcanzado un alto grado de trascendencia a nivel global y en diferentes campos, uno de ellos tiene que ver con la crisis hospitalaria que se vive mundialmente por el Covid-19, a raíz del importante impacto que tuvo la expansión del virus y la necesidad de aislamiento social, los mecanismos digitales se convirtieron en los mejores aliados para la continuidad de la actividad económica y social de los países en todo el mundo.

De acuerdo con el monitoreo de la Unión Internacional de Telecomunicaciones (UIT, 2021), organismo especializado de las Naciones Unidas en tecnologías de la información y las comunicaciones, para el 2005 había un 17% de usuarios de internet, por su parte en el 2010 se registró un 29%, más adelante en el 2015 se alcanzó un 41%, mientras que para enero de 2020, el 54% de la población mundial eran usuarios activos de medios tecnológicos, aproximadamente 4.100 millones de personas estaban online, en ese mismo año para el mes de abril, esta cifra incremento al 59%, correspondiente a 4.570 millones de personas. Estas cifras resultan cada vez más significativas para la toma de decisiones y direccionamiento en general de los mercados internacionales, y por ende en lo que respecta a mecanismos de defensa y mitigación de fraudes cibernéticos.

2. Antecedentes del problema

Para establecer un antes del problema que significa el robo virtual se debe establecer que el origen de esta metodología de fraude electrónico “Phishing” este dado por su traducción al español “pesca”, en este sentido y haciendo la analogía, se fundamenta en la preparación del “anzuelo” para lograr engañar a la víctima, esperando a que pique.

En la década de los 70 se consolido un importante movimiento entorno a los ataques de baja tecnología para la explotación de los sistemas telefónicos de la época, según un estudio “estos primeros hackers se llamaban “phreaks”, una combinación de las palabras inglesas “phone” (teléfono) y “freak” (raro, friqui). En una época en la que no había demasiados ordenadores en red que hackear, el phreaking era una forma común de hacer llamadas gratuitas de larga distancia o llegar a números que no salían en los listines” (Malwarebytes, 2020). Después de algunos años se empezaron a dar a luz situaciones fraudulentas en diferentes sectores, que relacionaban las metodologías y mecanismo que arraigaban el delito al concepto de phishing. Sin embargo, “la creación del término se atribuyó a un conocido spammer y hacker de mediados de los años 90, Khan C Smith” (Malwarebytes, 2020).

El término *“phishing”* traduce al español lo que se conoce como pesca, según Agrawal, Tewari, & Jain (2016); la palabra "phishing" fue utilizada por primera vez en Internet por un grupo de piratas informáticos en 1996, quienes robaron cuentas de América Online (AOL) engañando a los usuarios para que revelaran sus contraseñas.

Este término es adoptado para hacer alusión al robo de identidad automatizado mediante el cual se engaña a un grupo de personas, con el fin de obtener sus datos confidenciales y obtener provecho económico.

Esta metodología se fundamenta en la ingeniería social, “una herramienta de manipulación psicológica (…) que influyó en multitudes de personas durante la Segunda Guerra Mundial para salir y comprar bonos de guerra (…) lo que hace, es aprovechar la psique humana al explotar emociones poderosas como el miedo, la urgencia, la curiosidad, la simpatía o el sentimiento más fuerte de todos” (Zamora, 2021) y esto lo saben los ciberdelincuentes, quienes encuentran al usuario o en otras palabras al recurso humano, como el eslabón más débil o susceptible de una cadena tecnológica.

Es claro que cuando un usuario se enfrenta a un robo online como lo es el *phishing,* tiende a pensar que es más confiable una página que use nombres de entidades bancarias, puesto que su interfaz se presenta como sitio web legítimo y oficial.

En Colombia, existen un conjunto de normativas inmersas en el código penal que de cierta manera cobijan al usuario en el momento de ser víctima de este delito cibernético. En el código penal colombiano, el Artículo 269G se refiere expresamente a la suplantación de sitios web para capturar datos personales, definiéndolo como “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 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave” (Zabala A. , 2017, pág. 9)

Frente a este tipo de actos y la penalización por la ley colombiana, se comienza a hablar acerca de la responsabilidad que las entidades bancarias deben implementar en sus mecanismos de seguridad informática, para la protección de datos personales y/o financieros de sus usuarios y

así evitar que personas inescrupulosas tengan acceso a ellos, los suplanten y se materialicen riesgos relacionados con fraude, pérdida económica y deterioro de la imagen reputacional de las entidades bancarias.

Según Paiva (2021) argumenta que una vez desarrollado el punto de la vía jurídica por la que se debe analizar la responsabilidad que le incumbe al establecimiento bancario frente al fraude electrónico, es ahora oportuno revisar el elemento de causalidad o también conocido como el nexo de causalidad, en torno al "test de a causalidad en pasos" compuesto por dos segmentos, fáctico y jurídico, que da paso a la causa relevante del hecho.

Dicho esto, para cada acto que se cometa se debe tener en cuenta que tanto el usuario como la entidad pueden llegar a tener responsabilidad en generar un espacio propicio que permita la aparición de esta modalidad de robo cibernético.

3. Formulación del problema

El Phishing utiliza técnicas de ingeniería social que vulneran los modelos de seguridad informática de personas y entidades, logrando acceder a su activo más valioso, el cual, en este caso, será la información personal y financiera que de una manera u otra atentará en contra de su situación financiera. La falta de mecanismos de identificación de situaciones potencialmente fraudulentas para usuarios de plataformas tecnológicas de entidades bancarias se atribuye al desconocimiento tanto de las posibles técnicas relacionadas con este crimen cibernético, como a las estrategias utilizadas para la navegación confiable y segura a la hora de realizar transacciones en línea.

4. Pregunta problema de investigación

Teniendo en cuenta los antecedentes planteados y realizando la delimitación del problema que conlleva el *phishing*, haciéndose pasar por entidades bancarias para tomar ilegalmente información de personas del común con el fin de robar su dinero, se plantea como pregunta de investigación: ¿Cómo medir el nivel de vulnerabilidad de los usuarios y colaboradores de las entidades bancarias ante los ataques de phishing y establecer una metodología que permita prevenir a los usuarios frente a esta modalidad de robo?

5. Objetivos

5.1 Objetivo general

Analizar y diagnosticar la problemática que afectan a las diversas entidades bancarias hallando las herramientas o factores que usan para lograr la suplantación, luego de encontrar dichas falencias se pretende implementar un programa de inteligencia artificial que permita reducir o mitigar el robo de información de usuarios financieros en Colombia.

5.2 Objetivos específicos

- Realizar un estudio del arte de la vulnerabilidad informática como el phishing, con el fin de contextualizar, analizar, diagnosticar y proponer acciones que mitiguen el riesgo analizado.
- Establecer estrategias preventivas que aporten conocimiento para evitar ataques de cibercriminalidad basados en la teoría de la complejidad y la teoría del cambio en la gerencia de proyectos.

- Diagnosticar el sistema o proceso basado en los diferentes factores que se ven involucrados en suplantación encontrando patrones comunes con los cuales se desarrollan las estafas virtuales.
- Desarrollar un Modelo de Inteligencia Artificial y Machine Learning para identificar las diferentes formas de robo cibernético y postular estrategias para evitar ser víctimas de *Phishing.*

6. Justificación

La metodología de investigación abarca una serie de procedimientos aplicados de manera ordenada con el fin de dar validez y rigor a los estudios que se realizan, donde no solo se validan las causas sino los factores que influyen en dicha investigación con el fin de dar una explicación lógica al interrogante planteado. El desarrollo de esta investigación se llevará a cabo mediante un enfoque cuantitativo debido a que se recopilarán y se analizarán datos que permitan resolver el problema planteado.

En este sentido, la razón por la cual es viable escoger esta orientación, es porque "El enfoque cuantitativo utiliza la recolección de datos y el análisis de los mismos para contestar preguntas de investigación y probar hipótesis formuladas previamente, además confía en la medición de variables e instrumentos de investigación, con el uso de la estadística descriptiva e inferencial, en tratamiento estadístico y la prueba de hipótesis" (Ñaupa, Mejía, Novoa, & Villagómez, 2014, pág. 97).

Si bien es cierto, el phishing es una importante modalidad de robo cibernético que atenta contra la seguridad informática de los usuarios de internet, "los expertos coinciden en que el phishing sigue siendo un problema crucial que aún no ha sido resuelto. Esto se debe a que los

ataques de phishing están dirigidos a personas en lugar de máquinas" (Hindawi, 2022) convirtiéndose así en un problema social creciente que cada vez más toma fuerza debido a la era tecnológica en tanto que "los ataques de phishing afectan a más de 40 millones de usuarios de Internet cada año. Según un informe APWG (Antiphishing Grupo de trabajo), 15.208.832 sitios web de phishing y 103.347 correos electrónicos de phishing se detectaron en 2020. Además, las actividades de phishing alcanzaron su punto máximo en octubre de 2020 y 36.924 los ataques de phishing ocurrieron solo en enero de 2020" (Hindawi, 2022).

Por esto, la identificación teórica de cada una de las metodologías, servicios en los que tienen mayor nivel de influencia, relacionado con el modus operandi, se convierte en un importante elemento para el reconocimiento de estrategias que permitan determinar los diversos enfoques que se utilizan para mitigar estos ataques desde las áreas de acción. De la misma manera la consolidación de datos que permita medir, en términos generales, la percepción o conciencia de un grupo de personas acerca de este delito informático, ofrece un escenario de reconocimiento del nivel de vulnerabilidad y predisposición de usuarios de internet, en tanto que se definen variables claves relacionadas con Edad, ocupación, frecuencia de utilización de medios tecnológicos, entro otros elementos, que aportan la identificación del impacto a nivel social de este fraude tecnológico.

7. Marco Referencial

7.1 Antecedentes

Según Plazas (2018) se determinó que el usuario es el eslabón más débil a la hora de realizar un ataque de ingeniería social y que en los últimos años se han incrementado dichos ataques en las empresas colombianas ya que no invierten en herramientas seguridad informática, ni en las capacitaciones para los usuarios, por lo tanto, desconocen cómo deben actuar frente a un

ataque de ingeniería social. Adicionalmente afirma que el sector bancario es el más afectado utilizando la técnica de phishing.

El delito informático involucra diversas actividades criminales tales como lo son: los fraudes, falsificaciones, estafas, donde las redes sociales influyen en dichas falsificaciones ya que "los sistemas de redes sociales utilizan correos falsificados de empresas y agencias legítimas para permitir que los usuarios utilicen sitios web falsos para divulgar detalles financieros como nombres de usuario y contraseñas". (Dutta, 2021, pág. 1)

7.2 Marco teórico

7.2.1 Definición y modalidades de *Phishing*

El Phishing, este término es utilizado para referirse a uno de los métodos más utilizados de los delincuentes cibernéticos donde pueden obtener información confidencial de una forma engañosa donde pueden acceder a datos o información como lo son tarjetas de crédito o información relevante para acceder a sus datos privados, "esta es una forma de ingeniería social en la cual el atacante intenta adquirir fraudulentamente información substancial de una víctima haciéndose pasar por una organización confiable. (Jagatic et al., 2007).

Otra definición apropiada por Oxman (2013) es, añadiendo el término *Pharming,* el "*phishing*" y el "*pharming*" son dos tipos de fraudes informáticos que han aparecido desde mediados de la década pasada, cuya finalidad común es la de apoderarse de información personal de un usuario de Internet, para acceder a sus cuentas de correo o de redes sociales y obtener adicionalmente datos de sus contactos virtuales, a fin de comerciarlos ilícitamente, o bien, conseguir claves de *e-banking* para de este modo ingresar a las cuentas corrientes bancarias de los titulares y disponer del dinero que en ellas se encuentra, realizando una operación de transferencia de activos a un tercero que se denomina *mule* (en adelante, mulero o mula).

Como lo establece Rueda (2020), los ciberdelincuentes se valen de una gran variedad de ataques informáticos para lograr satisfacer sus deseos, en la actualidad existe un sin número de métodos, modalidades y programas maliciosos para llevarlo a cabo. Algunos requieren de más esfuerzo que otros y es por esto por lo que el phishing es tan apetecido por los delincuentes informáticos. El *phishing* y sus modalidades: a. *Smishing*, se describe como el engaño realizado por mensaje de texto; b. *Vishing*, engaño por medio de llamadas; c. *Spear-phishing*, ataques dirigidos y d. BEC, ataque dirigido a gerencia. Pueden utilizarse como un método único a la hora de robar datos confidenciales como primer paso, para finalmente robar dinero o si es deseo del ciberdelincuente puede utilizarlo como un medio para ejercer otro tipo de ataques informáticos, generalmente lo hacen cuando desean inyectar malware en el equipo informático. Dependiendo el malware que instalen será el daño que causen.

7.2.2 Ciberdelincuentes o *Phishers*

Los *pisher* más conocidos como el estafador o estafadores se valen de algunas técnicas de ingeniería social donde por medio de estrategias de mercado o información de interés social se hacen pasar por una empresa o persona de confianza donde aparenta una comunicación oficial mediante un correo electrónico o algún sistema de mensajería de respuesta rápida, a través de un programa donde a través de un enlace logra que el usuario ingrese sus datos y logra sacar sus credenciales o sus cuentas del banco. (Hadnagy, 2010)

Otra definición adjudicada a los *Phishers* según el Instituto Nacional de Ciberseguridad de España (2017) es, “el estafador o *phisher* suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador”.

Cabe señalar que los *phishers* se están volviendo más inteligentes. Siguiendo las tendencias en otros delitos en línea, es inevitable que las futuras generaciones de ataques de phishing incorporen mayores elementos de contexto para ser más efectivos y, por lo tanto, más peligrosos para la sociedad. Por ejemplo, supongamos que un *phisher* puede inducir una interrupción del servicio a un recurso utilizado con frecuencia, por ejemplo, para bloquear la contraseña de una víctima al generar fallas de autenticación excesivas. El *phisher* podría notificar a la víctima de una "amenaza de seguridad". Tal mensaje puede ser bienvenido o esperado por la víctima, que luego sería fácilmente inducida a revelar información personal. (Jagatic et al., 2007).

7.2.3 Alcances e impacto del *Phishing*

El *phishing* consiste en el manejo de mensajes donde por medio de estrategias de mercado o información de interés social se hace pasar por una empresa o persona de confianza, donde aparenta una comunicación oficial mediante un correo electrónico o algún sistema de mensajería de respuesta rápida, por ejemplo, entidades bancarias, spam, correo electrónico y correos masivos. Esto funciona a través de un programa donde a través de un enlace logra que el usuario ingrese sus datos y logra sacar su información, credenciales y sus cuentas bancarias.(Rodriguez-Corzo et al., 2018)

Con el pasar del tiempo a raíz del desarrollo tecnológico, los bancos han venido evolucionando su sistema con el fin de brindar un mejor servicio y facilitar muchas operaciones a todos sus usuarios.

En investigaciones realizadas por la universidad católica evidenciaron que “Colombia no ha sido ajena al proceso de incorporar nuevas tecnologías en sus operaciones financieras. En la década de los 70´s, los colombianos realizaban sus transacciones financieras con el efectivo,

cheque y en casos de élite con tarjeta de crédito, posteriormente en la década de los 80's llegan las transacciones con cajeros electrónicos y el uso de tarjetas débito y datáfonos para realizar pagos, esto enmarcado en una oferta de servicios reducida para un sector exclusivo de la sociedad" (Gómez, Mantilla, & Romero, 2018).

Como lo asegura Asobancaria (2020) frente al *phishing* en Colombia, "las campañas de *phishing* y *smishing* no son un tema exclusivo de países de economías desarrolladas y las acciones jurídicas y penales contra los cibercriminales depende de los marcos legales de cada país, por lo cual la adhesión a convenios internacionales y la inclusión de estas actividades como punibles en códigos son desde luego avances importantes. No obstante, también es fundamental que los gobiernos enfoquen sus esfuerzos en comunicarle a los ciudadanos los riesgos y precauciones que deben tener en cuenta al recibir mensajes o navegar por la web, siendo este un eje central en la prevención de dichos delitos".

7.2.4 Legislación en Colombia frente al *Phishing*

Ojeda, Rincón, Arias y Daza, argumentan que en Colombia, a partir de la Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos.

Medina, Cárdenas y Mejía (2021) aseguran que, Ley 1273 de 2009, De la protección de la información y de los datos". Dentro de los artículos 269A y siguientes, según la ley 1273 (2009) estos son: Artículo 269G: Suplantación de sitios web para capturar datos personales. 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 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. 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 la conducta no constituya delito sancionado con pena más grave. 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.

Cabe aclarar que, aunque literalmente los términos: "*Phishing*" e "Ingeniería social", no están contemplados en los artículos del código penal del 2009. Sus acciones delictivas, son las que irrumpen frente a la ley y ocasionen sanciones según su estado de acción. Ley 1298 de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

¿Cómo evitar estos ataques? Estos ataques se pueden evitar ignorando información de fuentes desconocidas, evitando diligenciar datos delicados como lo son sus cuentas bancarias, información personal y contraseñas, por otro lado, tener activado siempre el antivirus para estar alerta a cualquier amenaza ya que según Salcedo (2010) existen distintos mecanismos de defensa contra los phishing desarrollados en los últimos años. El primero de ellos consiste en el software de filtrado en los servidores de correo electrónico, encargado de eliminar los mensajes SPAM y que contengan software malicioso. Si el correo del *"phishing"* nunca llega a la víctima se habrá

reducido la vulnerabilidad inherente al factor humano. Sin embargo, los filtros anti-SPAM y el software antivirus no detienen el 100% de los no correos no deseados.

Por otro lado, también es importante evitar guardar contraseñas de acceso a diferentes plataformas en el navegador o en dispositivos personales, ya que, aunque pueda ser la opción más rápida para el usuario al momento de dar ingreso a cualquier plataforma debe tener en cuenta que es una manera mucho más fácil de que los ciberdelincuentes puedan obtener dicha información o incluso puede facilitar actos inescrupulosos tras hurto del dispositivo. Así como se deben tener ciertas precauciones al realizar transacciones bancarias ya que como lo hace saber Salcedo (2010) Realizar transacciones bancarias únicamente desde computadores confiables, es decir, cuyas condiciones de seguridad sean previamente conocidas. Evitar usar computadores de acceso público y en el caso de que no se tenga otra opción, asegurarse de borrar el historial de navegación, archivos temporales de Internet y apagar la computadora al terminar.

8. Marco Institucional

El sector en el cual se pretende enfocar el presente estudio es el bancario, conformado por "instituciones financieras que tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, con el objeto primordial de realizar operaciones activas de crédito" (La Hipotecaria, 2019). En este sentido, se pretende hacer un análisis de los resultados de niveles de vulnerabilidad y percepción que tienen los usuarios de entidades bancarias con respecto al phishing, siendo este tipo de entidades las más comunes en las metodologías de suplantación por medios electrónicos y sobre los cuales se deben identificar las principales estrategias de comunicación a sus usuarios para la

mitigación de los ataques cibernéticos a nombre de las entidades bancarias con las cuales utilizan algún tipo de servicio financiero.

Algunas de las tendencias más utilizadas por este tipo de entidades para la divulgación de información con respecto a los ataques cibernéticos, estás enmarcados en las publicaciones en las páginas oficiales, desde donde normalmente los usuarios realizan el ingreso de datos para transacciones en línea. Sin embargo, las denuncias presentadas cada vez se incrementan y se presentan como un importante campo de acción y decisión de la en cuanto a seguridad informática y responsabilidad respecto a los intereses económicos de sus clientes y de la comunidad en general.

9. Enfoque de la investigación

De acuerdo con Hernández, Fernández y Baptista (2014), el enfoque cuantitativo está basado documentos como los de Auguste Comte y Émile Durkheim. La investigación cuantitativa considera que el conocimiento debe ser objetivo, y que este se genera a partir de un proceso deductivo en el que, a través de la medicación numérica y el análisis estadístico inferencial, se prueban hipótesis previamente formuladas. Este enfoque se comúnmente se asocia con prácticas y normas de las ciencias naturales y del positivismo.

El enfoque cualitativo, está basado en el pensamiento de autores como Max Weber. Es inductivo, lo que implica que utiliza la recolección de datos para finar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación como lo mencionan Hernández, Fernández y Baptista (2014).

A diferencia de la investigación cuantitativa, que se basa en una hipótesis, la cualitativa suele partir de una pregunta de investigación, que deberá formularse en concordancia con la

metodología que se pretende utilizar. Este enfoque busca explorar la complejidad de factores que rodean a un fenómeno y la variedad de perspectivas y significados que tiene para los implicados.

La investigación cualitativa considera que la realidad se modifica constantemente, y que el investigador, al interpretar la realidad, obtendrá resultados subjetivos; se realiza a través de diferentes tipos de datos, tales como entrevistas, observación, documentos, imágenes, audios, entre otros.

Como enfoque principal de la investigación y basando la metodología de recolección de datos, lo que se desea es tener una percepción de los encuestados frente al tema de la investigación, en este caso, el *Phishing,* puesto que este concepto no tiene la suficiente visibilidad por parte de los medios audiovisuales colombianos e incluso las mismas entidades bancarias.

En ese orden de ideas, en esta investigación se toma un enfoque cualitativo con la finalidad de realizar una recolección de datos a una muestra poblacional del común que tenga o haya tenido lazos con entidades bancarias, haya realizado trámites, tenga cuentas activas o depósitos al interior de cualquier entidad. Mediante la aplicación de una encuesta se preguntará al usuario si conoce acerca del *Phishing,* lo que debe hacer y verificar antes de caer en esta modalidad de robo y las responsabilidades que posee la entidad frente a posibles suplantaciones.

10. Diseño y alcance de la investigación

Para esta investigación se tiene un diseño en cuatro etapas con las cuales, de manera lineal se quiere proponer una alternativa tanto para usuarios como para las entidades frente a la prevención y control de la suplantación de plataformas virtuales de entidades bancarias más conocido como *Phishing.*

1. Antecedentes: Antes de diseñar la encuesta es necesario establecer qué se ha investigado alrededor del *Phishing,* qué información se obtiene alrededor del tema y en Colombia cómo se ha manejado esta modalidad de robo.

2. Diseño de encuesta: Se procede a realizar una encuesta en la que se apunte a obtener información sobre la percepción de la población frente al tema de investigación, con ello se pueden establecer puntos con los cuales se proceda a proponer una alternativa para la prevención de esta modalidad de robo cibernético.

3. Recolección de datos: Mediante la encuesta aplicada a una muestra poblacional variada que tenga en común el acceso a entidades bancarias, lazos con las mismas o cuentas en diferentes entidades, sea usuario de alguna entidad; etc. Se realiza la consolidación de los datos por medio de Excel y se procede a la cuarta etapa.

4. Análisis de datos recolectados: Utilizando gráficos de los datos recolectados se hacen afirmaciones basadas en los resultados obtenidos con las cuales se desarrolle una opción de prevención que resuelva la pregunta de investigación y cumpla con el objetivo de la misma.

Teniendo en cuenta el diseño, el objetivo de la investigación y los datos que se desean recolectar, se establece como alcance de la investigación, conocimiento y percepción del usuario del común frente al *Phishing,* en entidades bancarias e información acerca de la prevención de esta modalidad de hurto por medio de internet. Con este alcance lo que se desea es establecer una serie de alternativas de protección, prevención y denuncia, tanto para el usuario bancario o persona natural, y las propias entidades que ofrecen el servicio o producto a sus clientes.

11. Variables objeto de la medición

Según el artículo “las variables”, publicado por la escuela de educación de la universidad Andrés Bello (2022), las variables pueden ser definidas como todo aquello que va a ser medido, controlado y estudiado en una investigación o estudio. Por consiguiente, es relevante, antes de iniciar una investigación, saber las variables que van a ser medidas y la manera en que se efectuará. En otras palabras, las variables deben ser susceptibles de medición. Variable es todo aquello que puede asumir diferentes valores, desde el punto de vista cuantitativo o cualitativo. (Bello, A., 2022)

Las variables pueden ser definidas conceptual y operacionalmente. La definición conceptual hace referencia a la teoría, mientras que la operacional nos da las bases de medición y la definición de los indicadores. Para definir las variables, debemos basarnos en los indicadores, que construyen el conjunto de actividades o características propias de un concepto. Para dar un ejemplo, podemos hablar de la inteligencia, la cual está compuesta por una serie de factores como la capacidad verbal, capacidad de abstracción, etc. Cada factor puede ser medido a través de indicadores. Dicho de otra manera, los indicadores son algo específico y concreto que representan algo más abstracto o difícil de precisar. No todos los indicadores tienen un valor similar. Es decir, aunque haya varios indicadores para un mismo concepto.

Tipos de variable:

1. Según sus propiedades matemáticas.
2. El criterio metodológico, y;
3. El nivel de medición de la variable.

El modelo utilizado en la estimación presenta una variable dependiente ya que esta se ejecuta con el fin de obtener un resultado que estime el estudio que se está realizando para poder

obtener la interpretación y así poder hallar los factores que determinan que un banco tenga la característica "*eventos a la seguridad digital*". Lo anterior con el objetivo de determinar si el factor asociado aumenta o disminuye la probabilidad de ocurrencia del evento.

12. Muestreo poblacional, técnicas de medición y tamaño de la población

Para esta investigación se realizó una encuesta de muestreo que según Galindo (1998) El valor del muestreo radica en la posibilidad de conocer el comportamiento de una población infinita, a partir de un subconjunto. Este procedimiento aporta una valiosa solución: sin necesidad de realizar un censo, es decir la observación o medición de todos los individuos de una población, podemos conocer las características que nos interesan.

Con la idea de poder ejecutarla se tomará un pequeño grupo de la población para aplicar la encuesta en mención, es mucho más pequeña que la población considerada y permite ejecutarse de manera más sencilla obteniendo así resultados más rápido, dicho lo anterior se tomará una población de sesenta y seis (66) personas las cuales deberán contar con dos características fundamentales para poder realizar la ejecución del muestreo

1. Personas desde los 18 hasta los 60 años y;
2. Que como requisito principal cuenten con productos financieros.

Ahora bien, con la información anterior la fórmula estadística para seleccionar una tasa de población para realizar encuesta es la siguiente:

$$\frac{n^1}{1+\frac{n^1}{N}} = n_1$$

Donde:

N: Tamaño de la población

n_1:Tamaño de muestra calculado

n^1: Tamaño provisional de la muestra dada por el investigador.

Y finalmente se estableció como técnicas de muestreo no probabilístico aleatorio que según Salinas (2004) su único requisito es cumplir con la cuota del número requerido de sujetos o unidades de observación. En este se desconoce la probabilidad de selección; tal es el caso de la participación de los voluntarios en un proyecto de investigación. La desventaja de este método es que no hay certeza de las diferencias entre las personas elegidas y el total de la población, por lo tanto, la generalizan a partir de los hallazgos de la muestra.

13. Modelo aplicado y técnicas organizacionales

Investigación cualitativa basada en los detalles de diseño observados en la campaña, los cuales darán un margen de precisión de la misma y hará que a futuro, pueda ejecutarse y obtener resultados objetivos acerca de la vulnerabilidad de los usuarios con productos y servicios financieros. La investigación parte del hecho de la importancia de la ciberseguridad en el mundo actual, ya que la información se encuentra en el ciberespacio y tanto personas como empresas son vulnerables a ataques que comprometen su información sensible, como cuentas, proyectos de investigación entre otros que podrían llevar a la quiebra de la misma (Williams et al., 2018).

14. Componentes y elementos funcionales de los modelos de la intervención

Como principales componentes y elementos dentro de la investigación de campo realizada, se toman en cuenta 3 principales que acompañan el proceso y que se vuelven cruciales en el momento de la recolección de datos para el análisis de la población entorno al tópico tocado en esta investigación.

14.1. Vulnerabilidad

Tabla 1.

Elementos de la investigación: Vulnerabilidad.

DENOMINACIÓN	VULNERABILIDAD
TIPO	Dependiente
NATURALEZA	Cuantitativa
MEDICIÓN	Estadística
INDICADOR	Número de personas que cayeron en el hacking
UNIDAD DE MEDIDA	Porcentaje
INSTRUMENTO	Base de datos
DIMENSIÓN	Estadística
DEFINICIÓN CONCEPTUAL	La vulnerabilidad informática es la debilidad en un sistema que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencias del sistema o de sus datos y aplicaciones. (Loja, 2011)

14.2. Personas

Tabla 2.

Elementos de la investigación: Personas.

DENOMINACIÓN	PERSONAS
TIPO	Independiente
NATURALEZA	Cualitativa
MEDICIÓN	Datos demográficos
INDICADOR	Edad, Sexo, Nivel de estudio, Énfasis
UNIDAD DE MEDIDA	Directa, Nominal
INSTRUMENTO	Datos demográficos
DIMENSIÓN	Social

DEFINICIÓN CONCEPTUAL	Según la RAE las personas son individuos que cuentan con derechos y obligaciones; ya en el ámbito tecnológico estas personas hacen parte de un sistema socio tecnológico que permite proporcionar un tratamiento unificado a los problemas de gestión de la innovación tecnológica y la intervención ambiental.(González García et al., 1996)

14.3. Encuesta

Tabla 3.

Elementos de la investigación: Encuesta.

DENOMINACIÓN	CAMPAÑA
TIPO	Independiente
NATURALEZA	Cualitativa
MEDICIÓN	Número de personas que denuncien el correo
INDICADOR	Efectividad de la campaña
UNIDAD DE MEDIDA	Ordinal
INSTRUMENTO	• Identificación de gráficos que sugieren clonación • Identificación de URL sospechosa
DIMENSIÓN	Numérica
DEFINICIÓN CONCEPTUAL	Según la RAE una campaña es "un conjunto de actos o esfuerzos de índole diversa que se aplican a conseguir un fin determinado."(Real Academia Española, 2016)

15. Instrumento para la recolección de la información

Para la recolección de información en curso, se realiza un cuestionario "modalidad de la técnica de la encuesta, que consiste en formular un conjunto de preguntas escritas, que están

relacionadas a hipótesis del trabajo y por ende a las variables e indicadores de investigación, su finalidad, es verificar la hipótesis de trabajo" (Ñaupas, Valdivia, Palacios, & Romero, 2018)

Cada una de las preguntas y secciones estructuradas, hacen referencia tanto al planteamiento como a la formulación del problema de la investigación, de la misma manera que pretende dar soporte a los objetivos generales y específicos previamente descritos.

La estructura del cuestionario inicia con la presentación de la institución y una breve explicación o introducción, "párrafo importante que sirve para explicar por qué y para qué se está aplicando el cuestionario, garantizando la confidencialidad y agradecimientos" (Ñaupas, Valdivia, Palacios, & Romero, 2018).

Se dan las instrucciones en donde se explican la escala de medición y/o calificación que se atribuirán a los planteamientos, que para el caso va de totalmente en desacuerdo a totalmente de acuerdo, es decir preguntas cerradas "aquellas en las que el encuestado escoge la respuesta adecuada a su punto de vista, dentro de un abanico de respuestas, pueden ser dicotómicas o politómicas" (Ñaupas, Valdivia, Palacios, & Romero, 2018).

Para este caso se para las tres primeras secciones, preguntas politómicas, "llamadas también de alternativa múltiple o de abanico, presentan tres, cuatro o más alternativas de respuesta" (Ñaupas, Valdivia, Palacios, & Romero, 2018). Mientras que para la última sección de conocimiento del encuestado se utiliza pregunta dicotómica, "solo se presentan dos alternativas para responder" (Ñaupas, Valdivia, Palacios, & Romero, 2018)

La información demográfica pertinente, para el caso, hace referencia a la ocupación del encuestado, en este sentido se pretende definir tanto el nivel educativo, como la relación del mismo con los medios tecnológicos y uso de medios electrónicos en la cotidianidad.

16. Técnicas y análisis de datos de acuerdo con el enfoque y diseño de la investigación

Para el análisis del modelo de recolección de datos se procede a realizar la tabulación para la consolidación de la información recolectada por medio de la encuesta de acercamiento en donde se tomaron en cuenta variables cualitativas enfocadas a la medición y reconocimiento de usuarios de entidades bancarias frente a la posibilidad y/o vulnerabilidad de ataques cibernéticos como el Phishing

La primera sección de la encuesta está dirigida al reconocimiento de ocupación de los encuestados, esto con el fin de medir los niveles de educación y/o posición, como un elemento clave para la determinación de comportamientos y utilización de plataformas para transacciones bancarias, ligado directamente al uso de medios tecnológicos a modo personal, laboral y de formación. En este sentido se identifica que el 39,39% corresponde a personal empleado, es decir que hace parte del sistema laboral del país y por ende posee algún servicio financiero; el 21% de los encuestados son estudiantes y el 4,55% son estudiantes y empleados.

Las ocupaciones relacionadas con cargos de asistentes, analistas, técnicos y tecnólogos representan un 18,18%, esto implica actividades laborales relacionadas con temas operativos y tácticos. A nivel profesional se identifica un 9% de los encuestados, relacionados con disciplinas de contabilidad, administración de empresas y gestión estratégico empresarial.

Tabla 4.

Recuento de ocupaciones de los encuestados.

Ocupación	Cant. Personas	Porcentaje
Administración de empresas	1	1,52%
Ama de casa	1	1,52%
Analista	2	3,03%
Asistente	3	4,55%

Auditor interno	1	1,52%
Cajera	1	1,52%
Contador público	2	3,03%
Coordinador	1	1,52%
Directora de servicio	1	1,52%
Empleado	26	39,39%
Enfermera	2	3,03%
Estudiante	14	21,21%
Estudiante/empleada	3	4,55%
Independiente	4	6,06%
Oficinista Cartera	1	1,52%
Técnico	3	4,55%
Total general	**66**	

Iniciando con la percepción de los encuestados frente a los canales de comunicación que existe entre las entidades bancarias y ellos como usuarios, se puede identificar qué el 32% de los encuestados, califican con 3, es decir ni en acuerdo ni en desacuerdo para para la medición de niveles de satisfacción al cliente, mientras que el 21% califica en desacuerdo y un 9% en total desacuerdo, esto en términos generales permite identificar la falencia o inconveniencia en los canales de comunicación que estas entidades tienen con sus usuarios

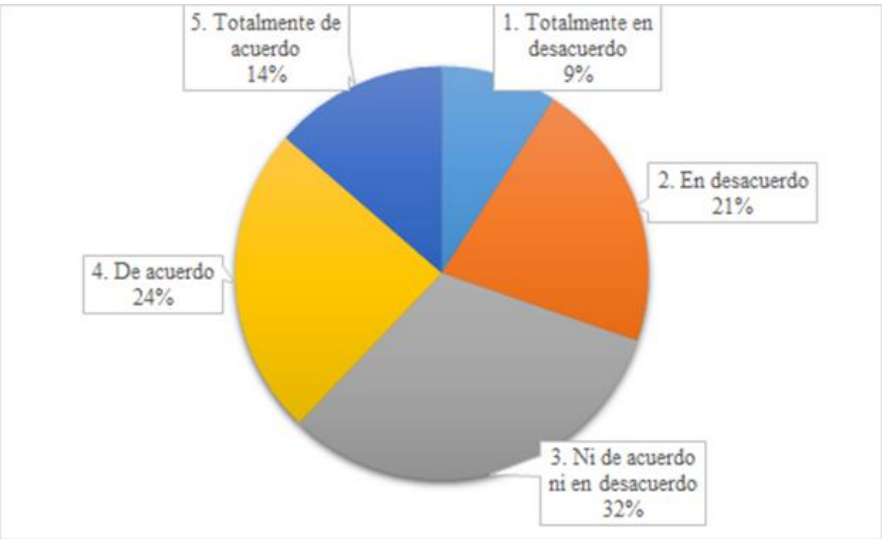
Tabla 5.

Consolidado posición sobre la satisfacción del cliente en las entidades bancarias.

¿La entidad donde tiene sus productos o cuenta bancaria mide constantemente el nivel de satisfacción del cliente?	
1. Totalmente en desacuerdo	6
2. En desacuerdo	14
3. Ni de acuerdo ni en desacuerdo	21
4. De acuerdo	16
5. Totalmente de acuerdo	9
Total General	**66**

Figura 1.

Porcentajes de posición de medición de satisfacción del cliente.



De la misma manera se puede identificar que la percepción de los encuestados frente a la ventaja competitiva dirigida al cumplimiento de las expectativas del cliente corresponde a un total de 15 respuestas entre totalmente en desacuerdo y en desacuerdo, para un 22% de los encuestados, mientras que un 35% afirma no estar ni en acuerdo ni desacuerdo. El 43% afirma estar de acuerdo y totalmente desacuerdo, lo que permite concluir que, si existe entre los usuarios encuestados de entidades financieras, una percepción positiva de ventaja competitiva.

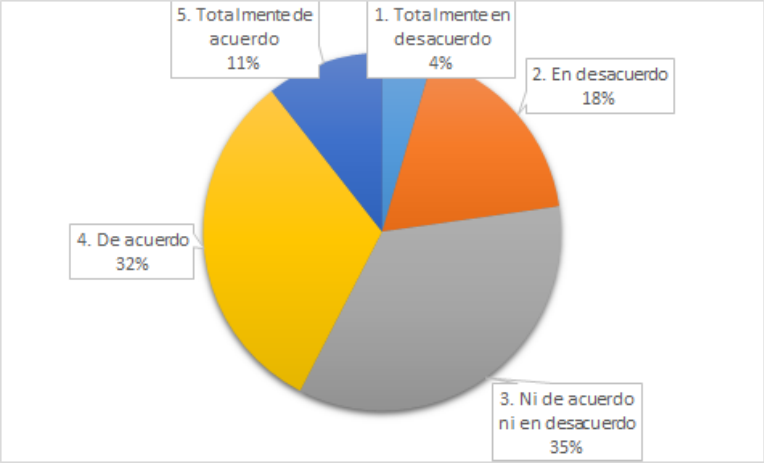
Tabla 6.

Ventaja competitiva de la entidad bancaria relacionada con el encuestado.

¿Considera que la entidad bancaria con la que tiene productos se caracteriza por tener ventaja competitiva basada en la comprensión de las necesidades de los clientes?	
1. Totalmente en desacuerdo	3
2. En desacuerdo	12
3. Ni de acuerdo ni en desacuerdo	23
4. De acuerdo	21
5. Totalmente de acuerdo	7
Total General	**66**

Figura 2.

Porcentaje de posición de la ventaja competitiva.



Por otro lado, en cuanto la comunicación de noticias relacionadas con ciberataque, y las estrategias que podrian evitar o mitigar los casos de delincuencia, se puede evidenciar que el 34% de los encuetados no tiene una percepcicón positiva, ya que califican entre totalmente en desacuerdo y en desacuerdo, ,a comunicación de dhica infromación por parte de la entidad, un 21% presentan una posición neutral, mientras que un 43% afirma estar de acuerdo y toalmente de acuerdo con la ejecución de estos canales.

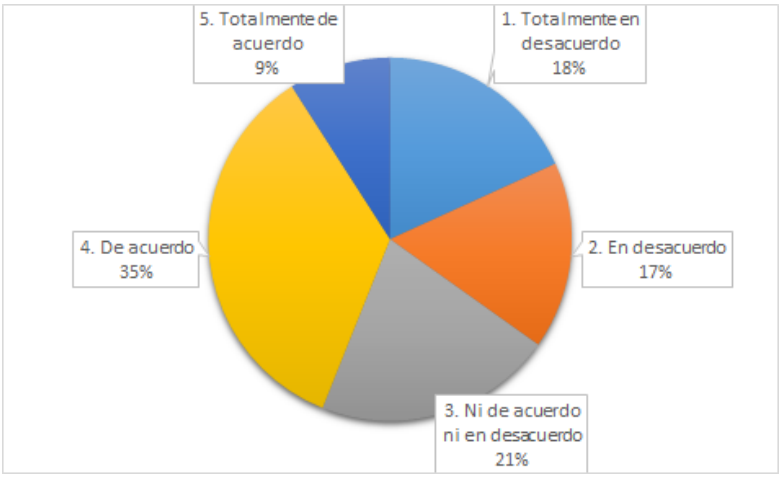
Tabla 7.

Conocimiento frente a la información de ciberataque otorgada por las entidades bancarias.

¿Dicha entidad comparte regularmente información sobre los casos de ciberataque y como el consumidor puede detectarlos y evitarlos?	
1. Totalmente en desacuerdo	12
2. En desacuerdo	11
3. Ni de acuerdo ni en desacuerdo	14
4. De acuerdo	23
5. Totalmente de acuerdo	6
Total general	**66**

Figura 3.

Porcentaje de acceso a la información anti delitos cibernéticos de entidades bancarias al usuario.



En cuanto a la planificación de estrategias para la disminución del riesgo y la percepción de los usuarios frene a ellas, se obtiene un resultado entre totalmente en desacuerdo y en desacuerdo de 13, para un porcentaje de 20%, mientras que un 36% no está ni en acuerdo ni en desacuerdo y un 44% afirma estar de acuerdo y totalmente de acuerdo con respecto a la planificación y ejecución de estrategias establecidas a nivel interno, que de una forma u otra pueden ser percibidas por los usuarios.

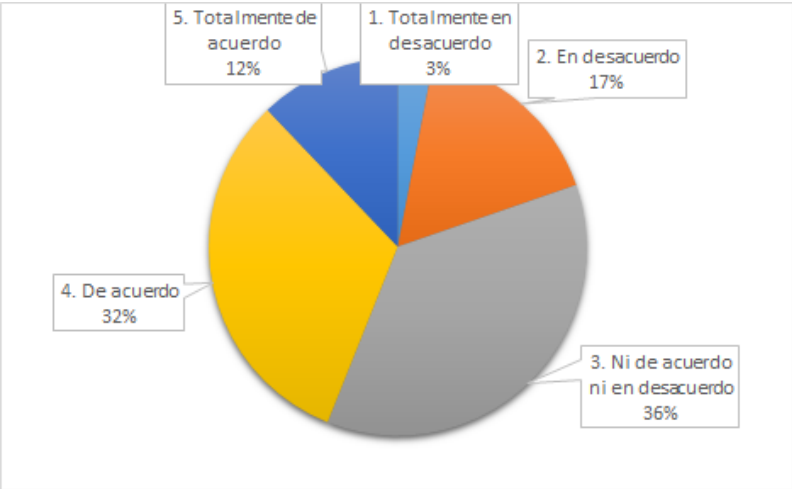
Tabla 8.

Planificación de estrategias *anti-Phishing* en entidades bancarias percibidas por usuarios.

¿Cree usted que allí se planifican y ejecutan estrategias que disminuyan el riesgo de phishing?	
1. Totalmente en desacuerdo	2
2. En desacuerdo	11
3. Ni de acuerdo ni en desacuerdo	24
4. De acuerdo	21
5. Totalmente de acuerdo	8
Total general	**66**

Figura 4.

Porcentaje de posición frente a estrategias *anti-Pshishing* en entidades bancarias.



Por otro lado, se obtiene un resultado de 72% entre totalmente de acuerdo y de acuerdo en cuanto a la importancia de la experiencia del cliente en las plataformas web destinadas para las transacciones en línea de entidades bancarias, para la determinación del nivel de satisfacción, solo un 10% afirma que este elemento no es importante para su experiencia en el servicio financiero.

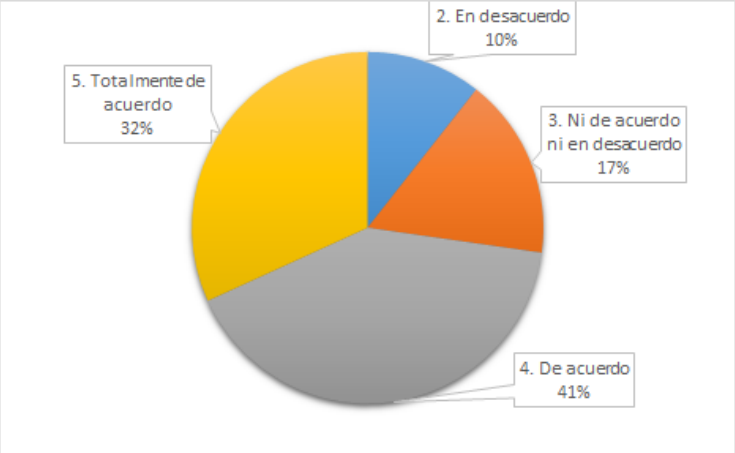
Tabla 9.

Consideración influencia entre satisfacción y lealtad de los usuarios en servicios transaccionales online.

Considera usted: ¿Qué la satisfacción con experiencias anteriores de uso de webs bancarias **influye positivamente en la lealtad hacia el uso de servicios bancarios online?**	
1. Completamente en desacuerdo	0
2. En desacuerdo	7
3. Ni de acuerdo ni en desacuerdo	11
4. De acuerdo	27
5. Totalmente de acuerdo	21
Total General	**66**

Figura 5.

Porcentaje de percepción de los encuestados en relación satisfacción y lealtad.



Otra de las secciones establecidas en el instrumento de recolección de información, está dirigida a la identificación de los usuarios de la responsabilidad o consciencia que las diferentes entidades bancarias deben tener respecto a los ataques cibernéticos y la garantía de la seguridad de la información personal y financiera de los usuarios, se puede identificar que un 92% de los encuestados están en acuerdo y totalmente de acuerdo con la necesidad de transmitir información constante acerca de cómo poder identificar y por ende evitar los fraudes cibernéticos.

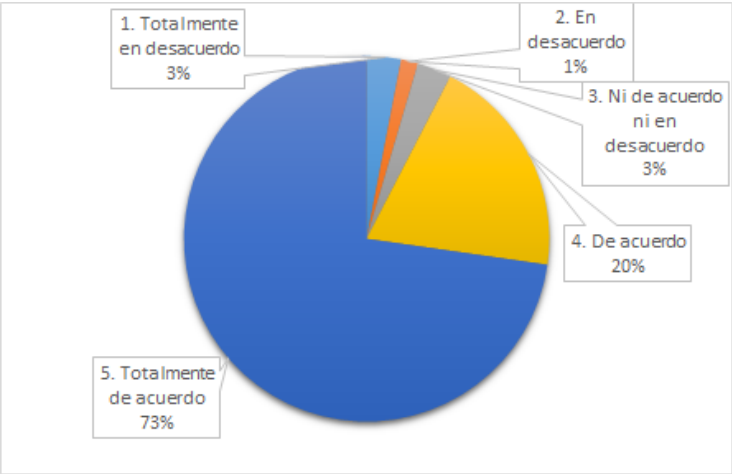
Tabla 10.

Importancia de la información al usuario sobre fraudes cibernéticos.

¿Considera que es importante que las entidades financieras brinden información al cliente sobre cómo evitar fraudes cibernéticos?	
1. Totalmente en desacuerdo	2
2. En desacuerdo	1
3. Ni de acuerdo ni en desacuerdo	2
4. De acuerdo	13
5. Totalmente de acuerdo	48
Total General	**66**

Figura 6.

Porcentajes de posición frente a la importancia de la información frente al fraude cibernético.



De la misma manera y muy alineado con la pregunta anterior, la priorización de estrategias puntuales para el tratamiento de fraudes cibernéticos incluidas en las políticas internas y que además garanticen la seguridad informática tanto de los usuarios como de las entidades, obtiene un porcentaje de importancia o aceptación dentro de los encuestados de un 90%, es decir que esto puede llegar a significar un elemento clave para la satisfacción del cliente.

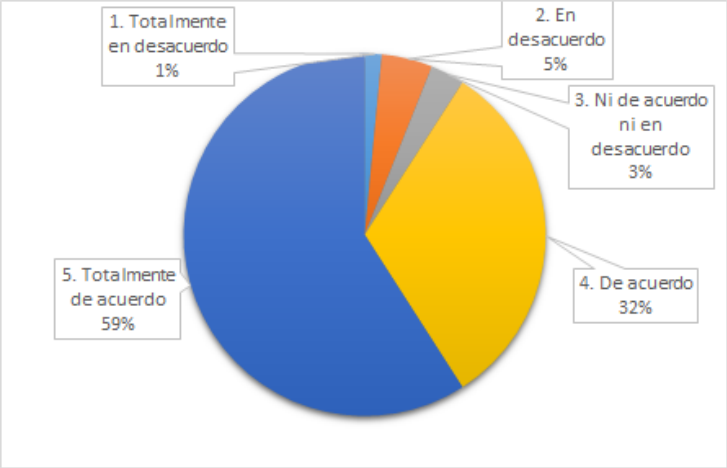
Tabla 11.

Priorización en las políticas internas frente a la prevención del *Phishing*.

Teniendo en cuenta los avances tecnológicos y los incrementos en ataques cibernéticos ¿Considera que las políticas internas de una compañía bancaria deben priorizar sobre estos aspectos?	
1. Totalmente en desacuerdo	1
2. En desacuerdo	3
3. Ni de acuerdo ni en desacuerdo	2
4. De acuerdo	21
5. Totalmente de acuerdo	39
Total General	**66**

Figura 7.

Porcentaje de posición frente a la adición de la prevención del *Phishing* en las políticas internas.



Un elemento importante relacionado con la capacidad tecnológica y la disposición de está para la atención de la necesidad del cliente, así como la percepción que se tiene sobre infraestructura de información, obtiene un 28% correspondiente a calificaciones de acuerdo y totalmente de acuerdo frente a la carencia de integración de recursos para la prestación del servicio, mientras que un 30% califican en desacuerdo y totalmente de en desacuerdo.

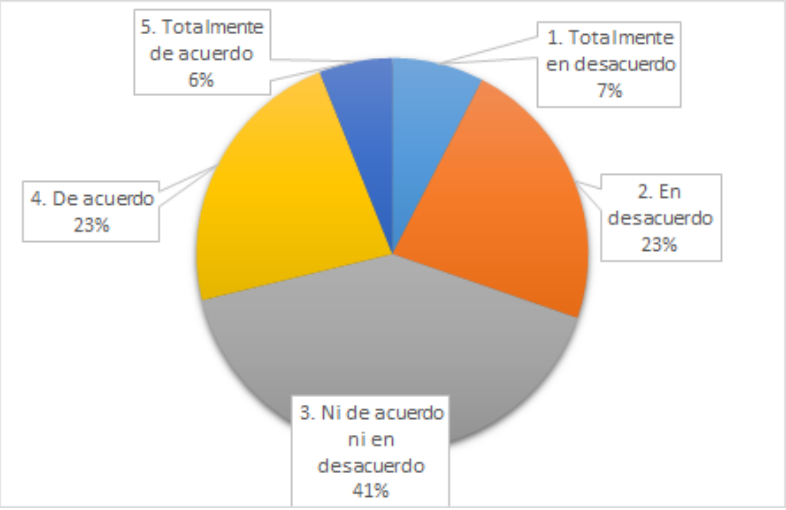
Tabla 12.

Consideración del encuestado frente a concepciones organizacionales.

¿Considera que la entidad donde tiene sus productos carece de factores importantes que influyen dentro de la integración como cultura organizacional, disponibilidad de recursos físicos y tecnológicos?	
1. Totalmente en desacuerdo	5
2. En desacuerdo	15
3. Ni de acuerdo ni en desacuerdo	27
4. De acuerdo	15
5. Totalmente de acuerdo	4
Total general	**66**

Figura 8.

Porcentaje de concepción del usuario frente a temas organizacionales de entidades bancarias.



Bajo la percepción de usuarios de entidades bancarias, se puede identificar que el 81% de los encuestados están de acuerdo y totalmente de acuerdo con la posibilidad y/o importancia de implementación de un área enfocada en el cumplimiento de exigencias legales, normativas y regulaciones vigentes para la reducción de fraude, así como la estructuración de experiencia al cliente fluida y segura, atendiendo a los crecientes niveles de ataques y fraudes por medio de la metodología phishing.

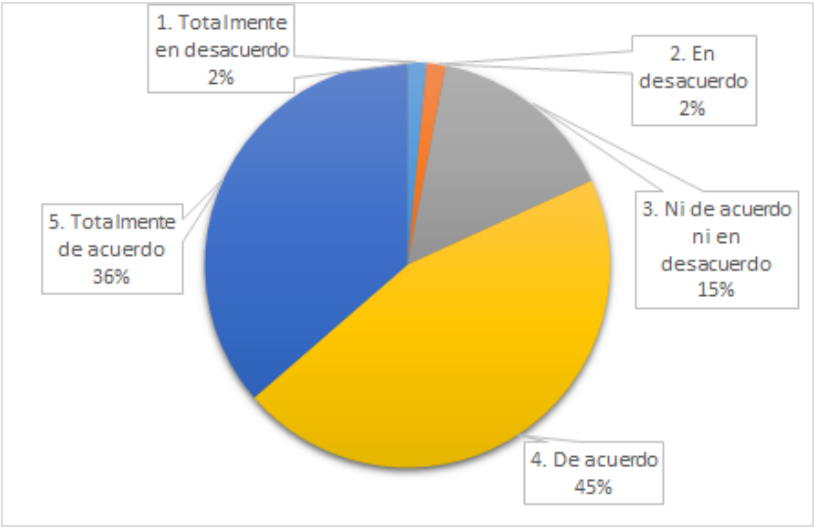
Tabla 13.

Adopción por parte de entidades bancarias de modelos antifraudes cibernéticos.

¿En su opinión, las entidades bancarias pueden adoptar un modelo de orientación en su área de AML o fraudes la cual pueda cumplir con los objetivos propuestos y así mismo satisfacer las necesidades de sus clientes de una manera segura?	
1. Totalmente en desacuerdo	1
2. En desacuerdo	1
3. Ni de acuerdo ni en desacuerdo	10
4. De acuerdo	30
5. Totalmente de acuerdo	24
Total general	**66**

Figura 9.

Porcentaje de adopción de modelos antifraudes cibernéticos en entidades bancarias.



Se pretende identificar los niveles de satisfacción de los usuarios frente al nivel de oportunidad de respuesta de las entidades bancarias en situaciones de fraude presentadas, con respecto a ello se obtiene un resultado de favorabilidad del 31%, mientras que un 14% está en desacuerdo o total desacuerdo en cuando a la reacción oportuna a eventos ocurridos.

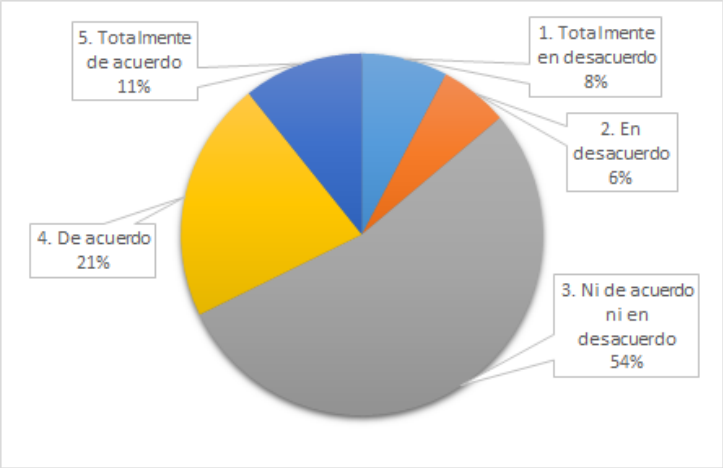
Tabla 14.

Actuación de las entidades bancarias frente al *Phishing*.

En caso de haber sido víctima **de *Phishing*, ¿considera usted que el establecimiento actuó a "tiempo" con el bloqueo de su producto al realizar estos el reconocimiento de un posible fraude por compras no frecuentes en clientes**	
1. Totalmente en desacuerdo	5
2. En desacuerdo	4
3. Ni de acuerdo ni en desacuerdo	35
4. De acuerdo	14
5. Totalmente de acuerdo	7
Total general	**65**

Figura 10.

Porcentaje posición de la actuación de entidades bancarias frente a posible *Phishing*.



El reconocimiento del mercado es importante para la identificación de estrategias a implementar en la mitigación del riesgo de fraude cibernético en las entidades bancarias, en este sentido se puede identificar que el 93% de los encuestados encuentran importante el reconocimiento por parte del consumidor de información relacionada con Phishing trayendo beneficios también a dicha entidad.

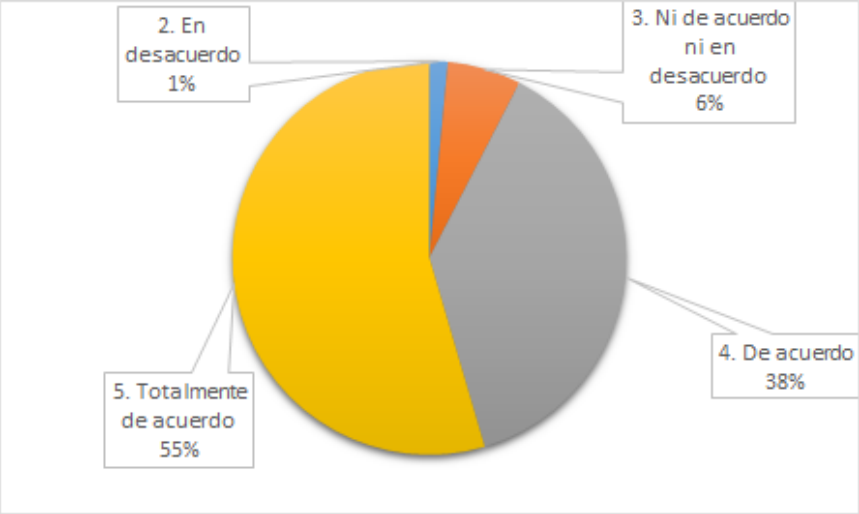
Tabla 15.

Orientación por parte de entidades bancarias a usuarios.

¿Considera que brindar la orientación pertinente al consumidor en temas de fraude puede beneficiar financieramente su compañía ante posibles pérdidas?	
2. En desacuerdo	1
3. Ni de acuerdo ni en desacuerdo	4
4. De acuerdo	25
5. Totalmente de acuerdo	36
Total general	**66**

Figura 11.

Porcentaje de encuestados posición de orientación de entidades bancarias a usuarios.



Este reconocimiento del mercado, es decir del comportamiento de los usuarios o clientes de entidades bancarias, está relacionado también con los modelos de desarrollo de innovación que puedan significar una estrategia puntual para los mecanismos de respuesta ante fraudes cibernéticos, en este sentido se obtuvo un porcentaje de favorabilidad frente a este planteamiento del 74%, es decir que al identificar características básicas del merado y del usuario permite establecer herramientas óptimas para los canales del servicio financiero que garanticen el cumplimiento de seguridad de la información.

Tabla 16.

Orientación al mercado en relación con la innovación.

Usted considera que la orientación al mercado se relaciona positivamente con consecuencias de innovación (Grinstein, 2008).	
2. En desacuerdo	1
3. Ni de acuerdo ni en desacuerdo	16
4. De acuerdo	28
5. Totalmente de acuerdo	21
Total general	**66**

Figura 12.

Porcentaje de posición frente a la relación orientación al mercado e innovación.

Debido a los crecientes casos de phishing, suplantación de identidad y en general de fraudes cibernéticos presentados en la actualidad, elementos de confianza y compromiso con la seguridad de los usuarios, empiezan a jugar un papel importante en la generación de ventaja competitiva en el mercado, y así lo perciben los encuestados, pues un 87% afirma estar de acuerdo y totalmente de acuerdo con este planteamiento.

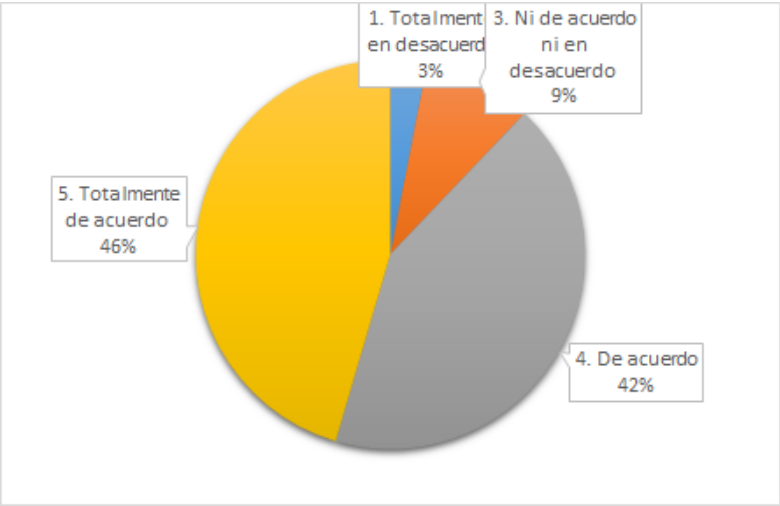
Tabla 17.

Confianza y compromiso como ventaja competitivas en el mercado.

¿Considera que las organizaciones deben identificar algunas variables como la confianza y el compromiso a sus clientes como un componente fundamental para lograr ventajas competitivas en la orientación al mercado?	
1. Totalmente en desacuerdo	2
3. Ni de acuerdo ni en desacuerdo	6
4. De acuerdo	28
5. Totalmente de acuerdo	30
Total general	**66**

Figura 13.

Porcentaje opinión de los encuestados relación confianza y compromiso como ventaja competitiva.



Por su parte, elementos como la protección de los datos, mecanismos para la mitigación del phishing y prácticas de buen uso de la información significan reducción en el impacto a nivel monetario tanto para los usuarios como para las entidades, dicha afirmación corresponde a un 92% que está en acuerdo y total acuerdo.

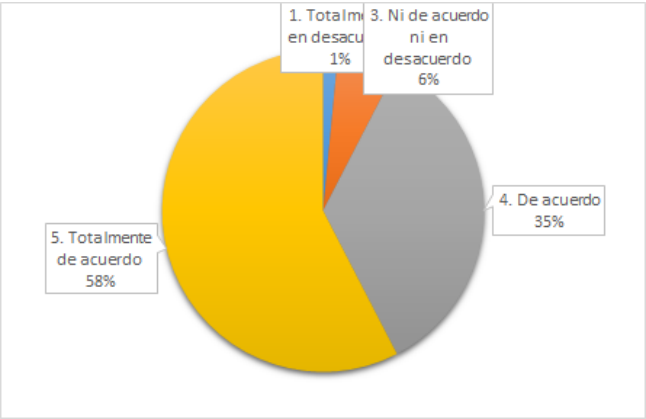
Tabla 18.

Protección de datos por parte de la entidad bancaria para evitar el *Phishing.*

¿Cree usted que la protección de datos, el conocimiento para evitar phishing y el saber dar buen uso a su información personal y financiera reduce notoriamente riesgos monetarios para usted y para el banco?	
1. Totalmente en desacuerdo	1
3. Ni de acuerdo ni en desacuerdo	4
4. De acuerdo	23
5. Totalmente de acuerdo	38
Total general	**66**

Figura 14.

Porcentaje opinión de los encuestados frente a la protección de datos por parte de las entidades bancarias.



Fuente: Elaboración propia.

La infraestructura interna en términos tecnológicos y de cumplimiento de promesa de valor al usuario, determina en gran medida el nivel de reconocimiento de capacidades claves para la consecución de estrategias dirigidas a la seguridad informática, y eso lo identifican os usuarios, con respecto a ello se identifica que el 20% están de acuerdo y totalmente de acuerdo con que las entidades donde tienen productos financiero, realmente cuentan con estas capacidades óptimas para dar respuesta oportuna a posibles fraudes cibernéticos, mientras que el 34% no está de acuerdo ni en desacuerdo, esto quiere decir que no es clara la identificación de estos recursos para la seguridad informática en su servicio.

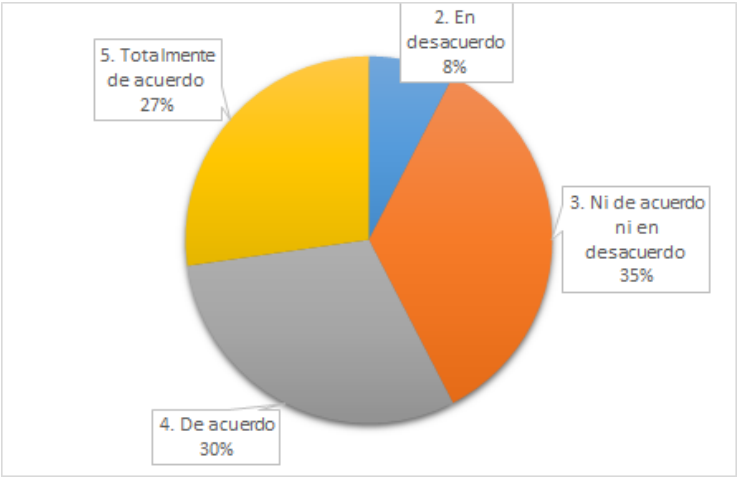
Tabla 19.

Entidades bancarias y sus capacidades tecnológicas para mitigar ataques cibernéticos.

De acuerdo con las respuestas anteriores, ¿La compañía en la que usted tiene sus productos financieros se encuentra en capacidades tecnológicas, innovadoras, culturales y organizacionales para mitigar en una parte considerable los ataques cibernéticos	
2. En desacuerdo	5
3. Ni de acuerdo ni en desacuerdo	23
4. De acuerdo	20
5. Totalmente de acuerdo	18
Total general	**66**

Figura 15.

Porcentaje de opinión del encuestado frente a las capacidades tecnológicas de las entidades bancarias a las que pertenece.



Finalmente, y con el fin de tener un conocimiento a nivel de utilización y de alguna manera vulnerabilidad percibida en los encuestados a ataque cibernéticos se realizan algunas preguntas relacionadas con el nivel de utilización de navegadores para transacciones bancarias, en donde 94% de la población encuestada afirma hacer uso de medios tecnológicos para estas transacciones. Por otro lado, se pretende determinar a nivel general de conocimiento de los usuarios tanto en temas de ataques cibernéticos, como de la reglamentación pertinente. En este sentido se observa que 62% si conoce cuáles son los deberes que las empresas financieras tienen en la protección de datos e información. En cuanto a las normas y requisitos legales, el 58% de los encuestados afirma conocerlos, mientras que el 42% no conocen la normativa referente a tratamiento de datos personales.

En cuento a la conciencia o precaución que se debe tener para la verificación de legitimidad e idoneidad de las páginas de entidades bancarias para la ejecución de transacciones en línea, bien sea consulta o transferencias, el 82% de los encuestados verifican previamente la

identidad de la página a la que acceden para estos fines, y solo el 30% tiene conocimiento acerca del procedimiento que se debe llevar a cabo en caso de ser víctima de un delito cibernético.

Tabla 20.

Preguntas de SÍ y NO frente a la posición del encuestado frente al *Phishing*.

¿Conoce cuáles son los deberes que tienen las entidades financieras en cuanto a la protección de datos e información formación personal y financiera de sus usuarios?		
NO	25	38%
SÍ	41	62%
Total general	**66**	
¿Usa navegadores u otras aplicaciones para sus transacciones bancarias?		
NO	4	6%
SÍ	62	94%
Total general	**66**	
¿Sabe cuáles son las normas y requisitos legales aplicables al tratamiento de datos personales en las entidades bancarias?		
NO	28	42%
Cuando realiza transacciones en línea bien sea por consulta u otras actividades relacionadas, ¿revisa la legitimidad de la página o plataforma a la que accede?		
NO	12	18%
SÍ	54	82%
Total general	**66**	
¿Sabe cuáles son las medidas que se deben tomar si llega a ser víctima de phishing?		
NO	46	70%
SÍ	20	30%
Total general	**66**	

El análisis Estadístico realizado a continuación, tiene como base el planteamiento de las siguientes hipótesis

H1. Todos los usuarios de plataformas bancarias donde se realizan transacciones en línea conocen los deberes de las entidades, relacionados con tratamiento y protección de datos

H2. La planificación y ejecución de estrategias para la disminución de riesghindawio de phishing por parte de las entidades influyen en la lealtad de los usuarios para el uso de servicios bancarios Online

H3. La integración de factores relacionados con cultura organizacional, disponibilidad de recursos físicos y tecnológicos influyen en el establecimiento de políticas internas teniendo en cuenta los avances tecnológicos

La correlación realizada para el análisis de la hipótesis H1, la cual es rechazada, presenta un coeficiente de 0,063 y no tiene porcentaje de confianza, en tanto que se determina que los usuarios de plataformas bancarias no tienen conciencia de los deberes que las empresas financieras tienen con respecto a la información y manejo de datos tanto personales como empresariales.

Tabla 21.

Cuadro de correlación 1

Correlaciones

		¿Usa navegadores u otras aplicaciones para sus transacciones bancarias?	¿Conoce cuáles son los deberes que tienen las entidades financieras en cuanto a la protección de datos e información formación personal y financiera de sus usuarios?
¿Usa navegadores u otras aplicaciones para sus transacciones bancarias?	Correlación de Pearson	1	,063
	Sig. (bilateral)		,613
	N	66	66
¿Conoce cuáles son los deberes que tienen las entidades financieras en cuanto a la protección de datos e información formación personal y financiera de sus usuarios?	Correlación de Pearson	,063	1
	Sig. (bilateral)	,613	
	N	66	66

Fuente: Elaboración propia

La relación directa que existe entre el nivel de percepción que tienen los usuarios, frente a la planificación y ejecución de alternativas que disminuyan el riesgo del phishing y la lealtad al uso de plataformas para transacciones en línea, obtiene una correlación de 0,327 con un nivel de confianza del 99%, por tanto, la hipótesis es aceptada y refleja el comportamiento positivo en la importancia que los usuarios le otorgan a las estrategias para disminución del riesgo para la lealtad de plas plataformas virtuales.

Tabla 22.

Cuadro de correlación 2

Correlaciones

		¿Cree usted que allí se planifican y ejecutan estrategias que disminuyan el riesgo de phishing?	Considera usted: ¿Qué la satisfacción con experiencias anteriores de uso de webs bancarias, influye positivamente en la lealtad hacia el uso de servicios bancarios online?
¿Cree usted que allí se planifican y ejecutan estrategias que disminuyan el riesgo de phishing?	Correlación de Pearson	1	,327**
	Sig. (bilateral)		,007
	N	66	66
Considera usted: ¿Qué la satisfacción con experiencias anteriores de uso de webs bancarias, influye positivamente en la lealtad hacia el uso de servicios bancarios online?	Correlación de Pearson	,327**	1
	Sig. (bilateral)	,007	
	N	66	66

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

Por su parte la identificación de factores influyentes en el modelo organizacional, en términos de cultura e integración tiene un comportamiento positivo con relación a la priorización de políticas internas teniendo en cuenta avances tecnológicos, al tener una correlación baja de 0,293 con un porcentaje de confianza de 95%, de esta manera

Tabla 23.

Cuadro de correlación 3

Correlaciones

		¿Considera que la entidad donde tiene sus productos carece de factores importantes que influyen dentro de la integración como cultura organizacional, disponibilidad de recursos físicos y tecnológicos?	Teniendo en cuenta los avances tecnológicos y los incrementos en ataques cibernéticos ¿ Considera que las políticas internas de una compañía bancaria deben priorizar sobre estos aspectos?
¿Considera que la entidad donde tiene sus productos carece de factores importantes que influyen dentro de la integración como cultura organizacional, disponibilidad de recursos físicos y tecnológicos?	Correlación de Pearson	1	,293*
	Sig. (bilateral)		,017
	N	66	66
Teniendo en cuenta los avances tecnológicos y los incrementos en ataques cibernéticos ¿Considera que las políticas internas de una compañía bancaria deben priorizar sobre estos aspectos?	Correlación de Pearson	,293*	1
	Sig. (bilateral)	,017	
	N	66	66

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia

Finalmente, se percibió una correlación importante de 0,628, con un porcentaje de confianza de 99% entre la importancia que los usuarios perciben en la identificación de variables relacionadas con confianza y compromiso, por parte de las entidades en donde tiene activos productos financieros, tiene comportamiento positivo con el impacto monetario que genera el conocimiento

para la prevención de ataques cibernéticos, así como el buen uso de la información tanto personal como financiera.

Tabla 24.

Cuadro de correlación 4

Correlaciones

		¿Considera que las organizaciones deben identificar algunas variables como la confianza y el compromiso a sus clientes como un componente fundamental para lograr ventajas competitivas en la orient...	¿Cree usted que la protección de datos, el conocimiento para evitar phishing y el saber dar buen uso a su información personal y financiera reduce notoriamente riesgos monetarios para usted y para...
¿Considera que las organizaciones deben identificar algunas variables como la confianza y el compromiso a sus clientes como un componente fundamental para lograr ventajas competitivas en la orient...	Correlación de Pearson	1	,628**
	Sig. (bilateral)		<,001
	N	66	66
¿Cree usted que la protección de datos, el conocimiento para evitar phishing y el saber dar buen uso a su información personal y financiera reduce notoriamente riesgos monetarios para usted y para...	Correlación de Pearson	,628**	1
	Sig. (bilateral)	<,001	
	N	66	66

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

17. Propuesta de solución para la prevención del phishing en entidades bancarias

Hoy por hoy, existen diferentes herramientas tecnológicas que permiten la automatización para el acceso a muchos productos financieros y como muestra de ello se puede observar las innovaciones que presentan muchas Fintech a nivel mundial que ayudan a mejorar la operación de forma flexible y mucho más segura. Es por eso que el uso de inteligencia artificial y Machine learning son una excelente oportunidad para la seguridad digital bancaria.

Debido a la cantidad de fraudes que se presentan por fuga de información de usuarios, es muy importante para las entidades financieras mantener la información confidencial y debidamente protegida, la implementación de esta tecnología artificial garantizaría seguridad en todos lo datos del usuario y en los movimientos transaccionales que este ejecute, este tiene el fin de saber con exactitud quien es la persona que está tratando de ingresar al sistema a través de los diferentes tipos de reconocimiento (facial, dactilar, entre otros).

De acuerdo a (Sosa, 2007), la Inteligencia Artificial se está aplicando a numerosas actividades realizadas por los seres humanos y se destacan entre otras las siguientes líneas de investigación científicas: La robótica, la visión artificial, técnicas de aprendizaje y la gestión del conocimiento. Estas dos últimas aplicaciones de la Inteligencia Artificial son las que más directamente se aplican al campo de las finanzas, debido a que en este campo existe una fuerte motivación orientada a la construcción de sistemas de información que incorporen conocimiento, y que permitan a los decisores de las organizaciones tomar decisiones.

Finalmente, como modelo de implementación para evitar ciberataques financieros, se concluye que esta tecnología artificial beneficia en general a toda la sociedad que cuente con

productos financieros y muchas de sus transacciones las realice digitalmente, ayudaría a reducir los altos niveles presentados anualmente por fraudes debido al robo de información.

Por consiguiente, se puede decir que con esta propuesta se pretende dar cumplimiento al objetivo de desarrollar un modelo de Inteligencia artificial que permita identificar los usuarios titulares del producto financiero con el fin de evitar el robo cibernético y evitar ser víctimas de *Phishing.*

17. Referencias

Asobancaria. (2020). *Impacto económico y social del phishing y el smishing en Colombia y el mundo.* Tomado de: https://www.asobancaria.com/wp-content/uploads/2020/10/1256VF.pdf

Agrawal, D. P., Tewari, A., & Jain, A. K. (2016). Fighting against phishing attacks: state of the art and future. *The Natural Computing Applications Forum*, 1.

Bello, U. A. (2022). Las variables. *Facultad de educación. Escuela de educación Andrés Bello*.

Caballero, M., & Cilleros, D. (2020). *Ciberseguridad y transformación Digital: Cloud, identidad digital, blockchain, agile, inteligencia atificial.* Madrid, España: Ediciones Amaya Multimedia.

Conoldo. (11 de Noviembre de 2021). *Conoldo: Uso estratégico de internwt para el desarrollo*. Obtenido de ¿Qué es una suplantación de identidad digital y cómo puede afectarte?: https://www.colnodo.apc.org/es/experiencias/que-es-una-suplantacion-de-identidad-digital-y-como-puede-afectarte

Dutta, A. K. (2021). Detecting phishing websites using machine learning technique. *Department of Computer Science and Information System, College of Applied Sciences, Almaarefa*, 1.

Galindo, L. (1998). *Biblioteca Marco, Técnicas de investigación en sociedad, cultura y comunicación. Mexico.* Obtenido de https://biblioteca.marco.edu.mx/files/metodologia_encuestas.pdf

Gómez, A., Mantilla, Y., & Romero, L. (2018). *Descripción del Desarrollo de la Banca Virtual en Colombia.* Bogotá D.C.: Universidad Catolica de Colombia.

Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. John Wiley & Sons.

Leguizamon, M. S. (2015). *Grado en Criminología y seguridad*. Obtenido de El phishing: http://repositori.uji.es/xmlui/bitstream/handle/10234/127507/TFG_Leguizam%c3%b3n_Mayra.pdf?sequence=1&isAllowed=y

Malwarebytes. (2020). *Acerca de Phising* . Obtenido de https://es.malwarebytes.com/phishing/

Manterola, C., & Otzen, T. (2017). *Técnicas de Muestreo sobre una Población a Estudio.* Obtenido de https://scielo.conicyt.cl/pdf/ijmorphol/v35n1/art37.pdf

Ñaupa, H., Mejía, E., Novoa, E., & Villagómez, A. (2014). Metodología de la Investigación Cuantitativa - Cualitativa y Redacción de la Tesis. 97.

Paiva, R. (2021). *El paradigma objetivo en la responsabilidad de las entidades bancarias por fraude electrónico: Una mirada desde las obligaciones de resultado*. Obtenido de https://repositorio.unal.edu.co/bitstream/handle/unal/80691/1033768750-2021.pdf?sequence=2&isAllowed=y

Plazas Garcia, E. R. (2018). *Ingeniería Social en las Empresas Colombianas.* Obtenido de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdfanteriorme

Portafolio. (2021). Alertan a entidades financieras sobre riesgos de suplantación. *Portafolio*.

Rodriguez-Corzo, J. A., Rojas, A. E., & Mejia-Moncayo, C. (2018). Methodological model based on Gophish to face phishing vulnerabilities in SME. In 2018 ICAI Workshops

Rodriguez , M. (2015). *Responsabilidad bancaria frente al phishing. Repositorio de la universidad Nacional*. Obtenido de https://repositorio.unal.edu.co/bitstream/handle/unal/57088/marcosrodriguezpuentes.2015.pdf?sequence=1&isAllowed=y

Salcedo, E. D. (2010). *Universidad de los Andes. Estudio de la Efectividad de Ataques de Phishing Sensibles al contexto. Obtenido de.* Obtenido de https://repositorio.uniandes.edu.co/bitstream/handle/1992/19174/u433133.pdf?sequence=1

Salinas, A. (2004). *Ciencia UANL. TEMA 4: Métodos de Muestreo.* Obtenido de https://www.redalyc.org/pdf/402/40270120.pdf

Sosa, M. d. (2007). *Inteligencia artificial en la gestión financiera empresarial. Universidad del Norte.* . Obtenido de https://www.redalyc.org/pdf/646/64602307.pdf

UIT. (2021). *Union internacional de Telecomunicaciones* . Obtenido de Stadistics Retrieved 2021: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Zabala, A. (2017). *Responsabilidad bancaria frente al delito de Phishing en Colombia*. Obtenido de Zabala, A. (2017). Responsabilidad bancaria frente al delito de phishing en Colombia. Tomado de: https://repository.ucatolica.edu.co/bitstream/10983/14943/1/Art%c3%adculo%20Phishing%20-%20Alexander%20Zabala.pdf

Zabala, A. (2017). *Responsabilidad bancaria frente al delito de Phishing en Colombia.* . Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/14943/1/

Zamora, W. (6 de Julio de 2021). *Malwarebytes*. Obtenido de Hackeando tu cabeza: cómo los ciberdelincuentes usan la ingeniería social: https://blog.malwarebytes.com/101/2016/01/hacking-your-head-how-cybercriminals-use-social-engineering/