UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

OCTUBRE 2024 - MARZO 2025

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

IMPACTO DE LAS TÉCNICAS DE PHISHING EN LA SEGURIDAD DE SITIOS WEB

ESTUDIANTE:

HECTOR EDUARDO SILVA CHICHANDE

TUTOR:

ING. JOSÉ DANILO VILLARES PAZMIÑO, MG.

AÑO

2025

I. PLANTEAMIENTO DEL PROBLEMA 6

II. JUSTIFICACIÓN 9

III. OBJETIVO DEL ESTUDIO 10

3.1. OBJETIVO GENERAL 10
3.2. OBJETIVOS ESPECÍFICOS 10

IV. LINEAS DE INVESTIGACION 11

V. MARCO CONCEPTUAL 12

5.1. DEFINICIÓN DE PHISHING 12
5.1.1. Concepto y características principales 12
5.1.2. Diferencias entre phishing y otras técnicas de ciberataque 13
5.1.3. Importancia de entender el phishing en el contexto actual de ciberseguridad 13
5.2. TIPOS DE PHISHING 14
5.2.1. Phishing tradicional: 14
5.2.2. Spear phishing 14
5.2.3. Smishing: 15
5.2.4. Vishing 16
5.2.5. Pharming 17
5.2.6. Whaling 17
5.2.7. Whishing 18
5.2.8. SIM swapping 19
5.2.8.1. Cómo funciona el SIM swapping 19
5.2.8.2. Medidas preventivas contra el SIM swapping 20
5.2.9. Qrshing 21
5.2.9.1. Cómo funciona el QRshing 21
5.2.9.2. Cómo protegerse del QRshing 22
5.2.10. Phishing de gemelo malvado 22
5.2.11. Pop-Up phishing 23
5.2.12. Phishing tipo Watering Hole 23
5.3. LA IMPORTANCIA DEL PHISHING PARA LA SEGURIDAD WEB 23
5.3.1. Usuarios 23
5.3.2. Organizaciones: 24
5.4. MEDIDAS DE SEGURIDAD EXISTENTES 24
5.4.1. Protocolos de autenticación 24
5.4.1.1. Autenticación de dos factores (2FA) 24
5.4.1.2. Captcha 24
5.4.2. Certificados SSL/TLS y cifrado de datos. 25
5.4.2.1. Certificados SSL/TLS 25
5.4.2.2. Cifrado de datos 25
5.4.3. Detección y Monitoreo de Actividades Maliciosas. 26
5.4.3.1. Monitoreo continuo 26
5.4.3.2. Sistemas de Detección de Intrusiones (IDS) 26
5.5. CONTEXTO EN ECUADOR 27
5.5.1. Escenario de Phishing en Ecuador. 27
5.5.2. Nivel de adopción de medidas de seguridad en sitios web locales. 27
5.5.3. Leyes y Regulaciones sobre Protección de Datos 27

VI. MARCO METODOLÓGICO 28

VII. RESULTADOS 29

VIII. DISCUSION DE LOS RESULTADOS 33

IX. CONCLUSIONES 35

X. RECOMENDACIONES 37

XI. REFERENCIAS 37

XII. ANEXOS 41

Tabla de ilustraciones

Ilustración 1 Como funciona el phishing ____ 12

Ilustración 2 *Correo Phishing ____ 14*

Ilustración 3 *Smishing ____ 15*

Ilustración 4 *desarrollo de un ataque de pharming* ***Fuente****: (Pharming, 2020) ____ 17*

Ilustración 5 *Pregunta 1 ____* ***¡Error! Marcador no definido.***

Ilustración 6 *Pregunta 2 ____* ***¡Error! Marcador no definido.***

Ilustración 7 *Pregunta 3 ____* ***¡Error! Marcador no definido.***

Ilustración 8 *Pregunta 4 ____* ***¡Error! Marcador no definido.***

Ilustración 9 *Pregunta 5 ____* ***¡Error! Marcador no definido.***

Ilustración 10 *Pregunta 6 ____* ***¡Error! Marcador no definido.***

Ilustración 11 *Pregunta 7 ____* ***¡Error! Marcador no definido.***

RESUMEN

En la actualidad, el crecimiento de internet y la digitalización de los servicios han traído grandes beneficios, pero también han abierto la puerta a nuevas amenazas cibernéticas. Entre ellas, el phishing se ha convertido en una de las técnicas más utilizadas por los ciberdelincuentes para engañar a los usuarios y obtener información confidencial, como contraseñas y datos bancarios. Este tipo de ataque no solo afecta a las personas, sino también a los sitios web, comprometiendo su seguridad y credibilidad.

El objetivo de este estudio es analizar cómo las distintas técnicas de phishing impactan la seguridad de los sitios web. A través de una investigación de tipo documental, se pretende identificar las estrategias más utilizadas por los atacantes, los métodos de defensa más efectivos y cómo estas amenazas han evolucionado con el tiempo.

A medida que las técnicas de phishing se vuelven más sofisticadas, es fundamental que tanto empresas como usuarios adopten prácticas de seguridad más robustas. La educación en ciberseguridad, la implementación de protocolos de autenticación avanzados y el uso de herramientas de detección de amenazas son aspectos clave para reducir el impacto de estos ataques. En este sentido, esta investigación no busca solo describir el problema, sino también contribuir con información relevante que ayude a mejorar la seguridad en entornos digitales.

El caso ecuatoriano es especialmente aterrador, ya que ha ocurrido un gran aumento en los ataques de phishing no solo a nivel mundial, sino también localmente.

Palabras clave

Phishing, ciberseguridad, ataques informáticos, ingeniería social, protección de datos, seguridad.

SUMMARY

Currently, the growth of the internet and the digitalization of services have brought great benefits, but they have also opened the door to new cyber threats. Among them, phishing has become one of the most used techniques by cybercriminals to deceive users and obtain confidential information, such as passwords and banking details. This type of attack not only affects individuals but also websites, compromising their security and credibility.

The objective of this study is to analyze how different phishing techniques impact website security. Through desk-based research, we aim to identify the strategies most commonly used by attackers, the most effective defense methods, and how these threats have evolved over time.

As phishing techniques become more sophisticated, it is essential that both companies and users adopt more robust security practices. Cybersecurity education, the implementation of advanced authentication protocols, and the use of threat detection tools are key aspects to reducing the impact of these attacks. In this sense, this research not only seeks to describe the problem, but also to contribute relevant information that helps improve security in digital environments.

The Ecuadorian case is particularly frightening, as there has been a significant increase in phishing attacks not only globally but also locally.

Keywords

Phishing, cybersecurity, computer attacks, social engineering, data protection, security.

I. Planteamiento del problema

Los usuarios y las empresas están cada vez más inseguros porque sus sitios web no han adoptado tecnología de seguridad que sea tan compleja como difícil de violar.

Más que molestos, mensajes disimulados como estas estafas de Internet son formas frecuentes de ciberdelito. Lo que realmente pretende hacer es extraer información importante de ti, como una contraseña o número de tarjeta de crédito; a veces incluso intentarán sacar unos cuantos dólares de sus víctimas.

Este tipo de delito no solo causa pérdidas económicas directas, sino que también daña la confianza del público en las víctimas y sus organizaciones. Así que la próxima vez que la gente me pregunte por qué me molesto en combatir esto, puedo decir simplemente eso: porque no te traerá más que problemas, algunos financieros, otros legales o regulatorios.

La nueva Directiva General de Protección de Datos de Europa, por ejemplo, significa que las organizaciones deben tomar medidas apropiadas para asegurar los datos privados. Si violan esta regla, entonces las sanciones relevantes serán muy severas, agregando una capa más de daño a las víctimas de un ataque de phishing.

Phishing significa un ataque a la tecnología informática que se aprovecha de mensajes maliciosos, por ejemplo, enviar correos electrónicos de Internet, noticias de exclusión, y sitios web falsos de phishing; el phishing implica engañar a las víctimas para que proporcionen información confidencial. Este tipo de ataque se caracteriza por encubrir su verdadera fuente como fuentes creíbles, tales como bancos, plataformas de comercio electrónico o grandes servicios en línea(*¿Qué es el phishing?*, 2022).

Entre las diversas tácticas de ingeniería social utilizadas por los atacantes, los atacantes utilizan diversos métodos de ingeniería social para ganar su confianza.

Entretanto, según un informe de la Organización de Estados Americanos sobre la ciberseguridad en el continente americano, los ataques de phishing son cada vez más preferidos y llevados a cabo por redes criminales bien organizadas, lo que aumenta enormemente su impacto.

El informe también señala que la tecnología de phishing evoluciona constantemente: puede imitar exactamente las páginas auténticas de sitios web; Con tecnología sofisticada, también puede eludir las medidas de seguridad diseñadas para proteger contra estos tipos de ataques. Es una amenaza que debe abordarse de manera integrada y efectiva, tanto a nivel institucional como individual (Sayago-Heredia, 2021).

Este ha sido un problema considerable durante algunos años (uno que ya tiene muchos problemas en nuestra sociedad), especialmente en lo que respecta a los ataques de phishing. Como resultado, las víctimas de ataques de phishing pueden tener que lidiar con aún más problemas, como tener que soportar delitos repetidos cometidos en su nombre o violaciones de datos personales de empleados y clientes de empresas que operan en el país. Las empresas ecuatorianas han pasado por alto la implementación regular de medidas preventivas y la capacitación en seguridad.

La situación es que, según estudios locales en Ecuador, más del 70 por ciento de las empresas no disponen de un mecanismo integral para protegerse de los ataques digitales. Esto se refleja principalmente en la vulnerabilidad de las empresas y organizaciones ecuatorianas en la web, ya que estas organizaciones son plataformas de comercio electrónico y partes de motores, etc. Han tomado todas las medidas imaginables para Esta amenaza no solo daña a las

organizaciones, sino también a los usuarios que visitan estos sitios web. Por ejemplo, cuando las personas ordenan mercancías que otras medidas de protección habrán adoptado a partir de 2024.

El objetivo es encontrar vulnerabilidades de seguridad generalizadas y fomentar buenas prácticas para defenderse contra estos ataques. Esto proporciona información útil para finalizar un estudio de caso en el presente y familiarizarse con las mejores prácticas de autenticación, la importancia de la tecnología de cifrado y el acceso en las organizaciones para el bienestar general del público en relación con el valor de la ciberseguridad.

Para permitir un estudio profundo y manejable, solo se analizarán los sitios web de empresas y organizaciones en Ecuador. Esto ciertamente ayudará a obtener datos concretos e investigar qué realmente constituye los niveles de vulnerabilidad y prácticas de seguridad y su evolución en el escenario ecuatoriano. Con estos hallazgos, se podrán proponer recomendaciones prácticas para reducir los riesgos de ataques de phishing en este país.

II. Justificación

Ya es hora de que implementemos medidas de seguridad fuertes en la web para proteger la información sensible de los usuarios y limitar el daño de las páginas de phishing. La aparición de este tipo de ataque cibernético se explica por la amenaza gradual que enfrentan los usuarios ecuatorianos con el proceso de digitalización acelerada en sectores sensibles, como el comercio, la educación y el gobierno. Ellos manejan cantidades significativas de datos personales y financieros: amplias oportunidades para el cibercriminal promedio.

Este estudio de investigación proporcionará información sobre el impacto del phishing en los sitios web de las organizaciones ecuatorianas y cómo identificarlos para el establecimiento de medidas de seguridad de acuerdo con el contexto local. También estás entrenando al país para hacer las mejores prácticas para proteger a los usuarios e instituciones.

Considerando que muchos de los sitios web en Ecuador aún no han agregado controles de seguridad básicos, se ofrecerá recomendaciones de investigación y soluciones prácticas que podrían reducir críticos estos riesgos. Además, la investigación se implementará junto con un módulo educativo para señalar la importancia de dar prioridad a la seguridad en Internet y crear una cultura organizacional de protección de la información.

El creciente uso de servicios digitales en Ecuador hace necesario entrar en un espacio cibernético más seguro, y este trabajo es parte de ese camino al proporcionar una caracterización detallada de las amenazas de phishing y cómo contrarrestarlas.

III. Objetivo del estudio

3.1. Objetivo general

- Evaluar el impacto de las técnicas de phishing en la seguridad de sitios web.

3.2. Objetivos específicos

- Establecer las medidas de protección de seguridad para prevenir ataques en sitios web
- Describir controles para los ataques phishing utilizados en los sitios web
- Proponer estrategias de seguridad para prevenir los ataques phishing en los sitios web

IV. LINEAS DE INVESTIGACION

Línea de investigación: Sistemas de información y comunicación, emprendimiento e innovación. Es por eso que, en cuanto a la frecuencia con que estas funciones ocurren e instancian compromisos con la seguridad de los sistemas de información, y por lo tanto en el estudio de los sistemas de información y comunicación, proporciona un análisis que reconoce el riesgo y luego identifica formas de mitigar dicho riesgo en los sitios. Lo mismo ocurre con el Emprendimiento y la Innovación, donde nuevas estrategias de detección y prevención resuenan con las nuevas tecnologías y el movimiento de protesta, fomentando una decodificación del inframundo cibernético, y una relación simbiótica entre la inteligencia artificial y la educación digital para promover la seguridad de la información.

Sublínea de investigación: Redes y tecnologías inteligentes de software y hardware.

Examinamos la relación entre el phishing y la impotencia de los protocolos, junto con la vulnerabilidad de los sitios web. Medios técnicos como hardware y software pueden así debilitar estos ataques: autenticación multifactor, filtrado de correos electrónicos y análisis de comportamiento mediante reglas. Los sistemas de reconocimiento de patrones de ataque y los beneficios del aprendizaje automático, combinados con inteligencia artificial basada en sistemas de detección de intrusos (IDS), se convierten en una excelente manera de minimizar el acceso a través de estafadores en línea.

V. MARCO CONCEPTUAL

5.1. Definición de phishing

5.1.1. Concepto y características principales

El phishing, actualmente, es una forma muy común de ciberataque y utiliza correos electrónicos, SMS y llamadas telefónicas para interceptar la comunicación de las personas. El objetivo es persuadir al receptor para que realice las acciones que se desean, por ejemplo, iniciar un acceso a una cuenta para interceptar información o recoger un número de tarjeta de crédito de otro usuario del sistema informático del banco. Un atacante se hará pasar por una parte confiable para engañar a las víctimas y causarles daño. Lo hacen haciendo clic en enlaces que los llevan a sitios maliciosos o descargando virus informáticos, y proporcionando direcciones de correo electrónico sensibles cuando se les pide llenar formularios por internet(*¿Qué es phishing?*, 2022).

Ilustración 1 Como funciona el phishing

Fuente: (¿Cómo identificar un correo electrónico de phishing?-Comunidad Huawei Enterprise*, 2024)*

5.1.2. Diferencias entre phishing y otras técnicas de ciberataque

- **Malware:** Malware es un término inclusivo utilizado para referirse a cualquier tipo de software malicioso diseñado para causar daño o conseguir acceso de forma secreta al ordenador de una persona desprevenida. Con campañas de phishing, gusanos, u otros medios de comunicación similares a través de la red —por lo general descargas no autorizadas de material de Adobe que se activan mediante un script— el malware puede instalarse en un sistema (*Tipos de malware y ejemplos*, 2017).

- **Ransomware**: Es una subclase de malware. La empresa bloquea a la víctima fuera de cualquier dato o sistema que también puede estar cifrado y después de esto exige el pago antes de que se pueda recuperar el uso. El phishing busca engañar a las víctimas para que envíen información personal secreta para lograr sus objetivos; sin embargo, tal estafa en este caso bloquea físicamente tu capacidad para operar como deseas y te impone la invasión de las reglas de otra persona(*¿Qué es el ransomware?*, 2024).

5.1.3. Importancia de entender el phishing en el contexto actual de ciberseguridad

Con el nivel de rutina de ataque sistémico y las personas que llevan a cabo phishing volviéndose cada vez más sofisticadas, nunca ha parecido más importante que ahora entender qué es el phishing en el clima moderno. Este tipo de ataque combina tanto el engaño por parte del estafador como algunas de las tecnologías más exquisitamente falsas en este lado del fraude. Tan fácilmente puede llevar a otros peligros serios, como razas de virus en un sistema interno o ransomware completamente desarrollado que entra a través de uno de esos phishes: pequeños gusanos donde antes había comodidad y seguridad (*¿Qué es un ciberataque y los tipos de ataques en la red?*, 2022).

5.2. Tipos de Phishing

El phishing se presenta en diversas modalidades, cada una con características específicas:

5.2.1. Phishing tradicional:

Esto implica enviar miles de correos electrónicos falsos que parecen auténticos y están dirigidos a una persona o empresa desde muchas fuentes, algunas elaboradas a mano, otras producidas en masa, para obtener información valiosa de las personas objetivo o manipularlas para hacer lo que el atacante desea (*¿Cuáles Son los Distintos Tipos de Phishing?*, 2021).

5.2.2. Spear phishing

Este tipo no solo está dirigido a muchos, sino que también es personalizado para cada objetivo. Los atacantes, después de aprender sobre la víctima, hacen que sus mensajes se ajusten más a este marco y, por lo tanto, son mucho más disciplinados que un enfoque arbitrario y único para todos. ¿El resultado? Muchos ataques exitosos ocurren(¿Cuáles Son los Distintos Tipos de Phishing?, 2021).

Ilustración 2 *Correo Phishing*

Fuente: *Elaboración Propia*

5.2.3. Smishing:

Utiliza mensajes de texto (SMS) fraudulentos para engañar a las víctimas y obtener información confidencial o inducirlas a realizar acciones perjudiciales (*¿Cuáles Son los Distintos Tipos de Phishing?*, 2021).

Ilustración 3 *Smishing*

Fuente: *(¿Qué es Smishing y cómo protegerse?, 2023)*

5.2.4. Vishing

Implica llamadas telefónicas en las que el atacante se hace pasar por una entidad confiable para obtener datos sensibles de la víctima (*¿Cuáles Son los Distintos Tipos de Phishing?*, 2021).

A menudo, el objetivo es obtener información adicional como:

- Llamada del banco: Cuando recibes una llamada de alguien que dice que es del departamento de seguridad del banco para que confirmes tus datos personales para resolver un problema con tu cuenta.
- Soporte técnico falso: Cuando recibes una llamada de alguien que dice ser del soporte técnico de una empresa conocida, para poder tener acceso a tu computadora para solucionar un problema.
- Fraude de impuestos: Cuando recibes una llamada de alguien que dice ser de alguna agencia tributaria y te amenaza con emprender acciones legales si no paga una deuda pendiente.

5.2.5. Pharming

Técnica en la que los usuarios son redirigidos desde sitios web legítimos a versiones falsificadas sin su conocimiento, generalmente mediante la manipulación del sistema de nombres de dominio (DNS). Esto permite a los atacantes recopilar información confidencial ingresada en estos sitios falsos (*¿Cuáles Son los Distintos Tipos de Phishing?*, 2021).

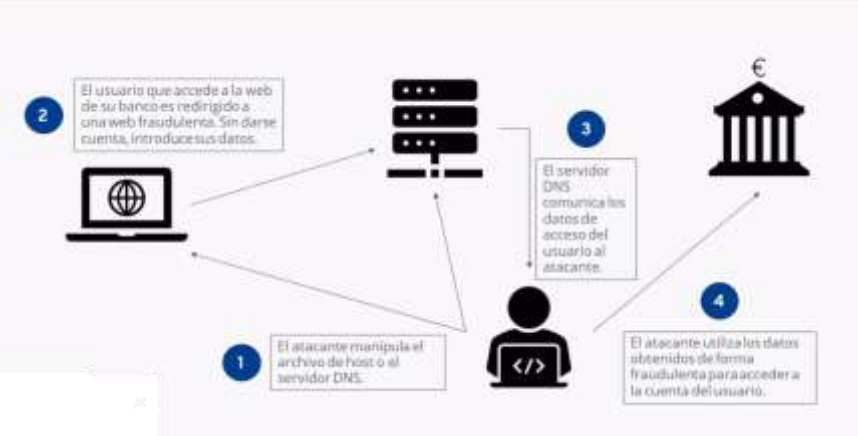

Ilustración 4 *desarrollo de un ataque de pharming*
Fuente*: (*Pharming*, 2020)*

5.2.6. Whaling

La caza de ballenas (whaling, en inglés) es cuando los ciberdelincuentes apuntan específicamente a altos ejecutivos o aquellos con acceso a información sensible de la empresa en una estafa de phishing. En estos ataques, los criminales se hacen pasar por una figura importante, por ejemplo, su CEO o CFO, para engañarlo y robar su información confidencial o autorizar transferencias fraudulentas(*¿Qué es el whale phishing?*, 2023).

5.2.7. Whishing

El término whishing el uso de técnicas de phishing a través de aplicaciones de mensajería instantánea, como WhatsApp todavía no se utiliza ampliamente en el mundo de la ciberseguridad. Pero los ciberdelincuentes pueden falsificar mensajes en WhatsApp. Y el contenido del mensaje puede ser de fuentes reputadas que conoces, como promociones de marcas conocidas o alertas de noticias sobre nuevos productos, lo cual siempre resulta atractivo en las redes sociales y está presente todo el tiempo. Su objetivo es cometer robo de información e infectar su dispositivo con un virus.

Para protegerse de estos ataques, puede considerar:

- No responder ni hacer clic en enlaces en mensajes de números desconocidos que pidan información personal o dinero.
- Antes de tomar cualquier acción, contactar al remitente por otros medios para verificar su autenticidad.
- No visitar enlaces sospechosos ni descargar archivos de fuentes no comprobadas.
- Tener siempre activa la seguridad en WhatsApp y, si hay algo sospechoso, reportarlo.

5.2.8. SIM swapping

El intercambio de SIM, también conocido como duplicación de SIM o suplantación de tarjeta SIM, no es un fraude nuevo. Un estafador adquiere un duplicado de la SIM de la víctima y luego se apodera de su número de teléfono. Una vez con la nueva SIM en mano, un atacante puede interceptar mensajes de texto, incluidos códigos de autenticación de dos factores, y desviar dinero de cuentas bancarias o extraer efectivo de otros lugares en el ciberespacio, según sea necesario(BBVA, 2025).

5.2.8.1. Cómo funciona el SIM swapping

- **Obtención de información personal:** El atacante recopila datos personales de la víctima, como nombre completo, dirección, número de teléfono y detalles de cuentas bancarias, a través de técnicas de ingeniería social o phishing (Campillo, 2022).
- **Contacto con la operadora de telefonía:** Con la información obtenida, el delincuente se comunica con el proveedor de servicios móviles de la víctima, suplantando su identidad.
- **La interceptación dañina de comunicaciones:** Tras llenar el formulario de cambio de operador, la víctima pierde el servicio temporalmente, pero a partir de ahora el atacante controla totalmente el número de teléfono de esta persona y puede recibir sus mensajes, llamadas, etc. Incluso podría interceptar códigos de verificación para servicios en línea (BBVA, 2025).

5.2.8.2. Medidas preventivas contra el SIM swapping

- Activar la autenticación en dos pasos (2FA): Utilizar aplicaciones de autenticación o llaves de seguridad físicas en lugar de depender únicamente de códigos enviados por SMS.
- Pedir al proveedor de telefonía establecer más precauciones: Algunas compañías ofrecen una opción de protección de cuenta, como establecer un PIN o contraseña para realizar cambios de SIM.
- Mantén la información personal confidencial: No publiques online aquella información que puedas ser especialmente vulnerable a ataques holísticos por terceras partes, ya sea a través de redes sociales o por canales poco confiables.

5.2.9. Qrshing

QRshing es un tipo de phishing en el que un atacante disfraza un código QR malicioso para robar la información privada o financiera de las víctimas. Cuando un usuario escanea un código QR comprometido, es dirigido a un sitio web falso que está configurado para robar datos sensibles de la víctima o instalar malware en su sistema con finalidad de infectar el dispositivo (*Quishing*, 2024).

5.2.9.1. Cómo funciona el QRshing

- Falsificación de códigos QR: Los estafadores crean sus propios códigos QR con la finalidad de redirigir a todos los usuarios que los escanean a sitios web no autorizados con contenido inapropiado uno tras otro.
- Áreas públicas: donde es más probable que la mayoría de las personas los vean, como restaurantes y estacionamientos, están ubicados aquí para un fácil escaneo.
- A sitios web inseguros: el usuario es llevado a un lugar que puede solicitar información privada o se puede descargar silenciosamente software malicioso en su computadora después de escanear el código.

5.2.9.2. Cómo protegerse del QRshing

- Mirar la fuente: antes de escanear un código QR, asegúrese de que su procedencia sea confiable.
- Evitar escanear en lugares dudosos: En espacios abiertos, no se deben escanear códigos QR a menos que se le indique que son seguros para escanear.
- Aplicaciones de escaneo seguras: Si estás usando aplicaciones para escanear algunos códigos QR regularmente, también deberías tener una aplicación de escaneo que tenga características de seguridad adicionales además de las convencionales y siempre asegurarte de verificar la URL que se abrirá.
- Mantén tu teléfono actualizado: Es necesario actualizar tu teléfono periódicamente para revisar y buscar vulnerabilidades conocidas, ya que todas las vulnerabilidades encontradas se corregirán con cada actualización.

5.2.10. Phishing de gemelo malvado

Los atacantes han desarrollado un virus llamado ataque de identidad gemela maliciosa, que crea un punto de acceso Wi-Fi falso que se parece mucho a la red real. Los usuarios se conectan sin saberlo a esta red falsa, su línea de comunicación es interceptada y toda la información es sustraída por personas cercanas (*¿Qué es un ataque de gemelo malvado y cómo actúa?*, 2023).

5.2.11. Pop-Up phishing

El phishing a través de ventanas emergentes se refiere a la creación de ventanas falsas que los ciberdelincuentes utilizan para engañar a un usuario y obtener algún beneficio de datos privados (inicio de sesión, financieros, etc.). También puede significar la instalación de malware en tu computadora. Estas ventanas emergentes no están tan alejadas de las notificaciones del sistema legítimas que recibes de los sistemas operativos, navegadores web o programas antivirus. Muestran información ficticia sobre amenazas y advierten al usuario que debe responder de inmediato (*Cómo identificar y eliminar ventanas emergentes falsas*, 2019).

5.2.12. Phishing tipo Watering Hole

En inglés, "water hole attack" es un tipo de ciberataque en el que los atacantes apuntan a un subconjunto determinado de usuarios comprometiendo primero un sitio web que un grupo de usuarios frecuenta. Infectarán estos sitios con malware para poder acceder a los sistemas de las víctimas si y cuando estas páginas sean visitadas (*What Is a Watering Hole Attack?*, 2021).

5.3. La Importancia del Phishing para la Seguridad Web

5.3.1. Usuarios

Qué Puedes Hacer Sobre el Phishing: los usuarios son engañados para que proporcionen información personal sensible, incluyendo detalles de inicio de sesión e información de tarjetas de crédito. Esto puede resultar en pérdidas económicas, robo de identidad y comprometer la privacidad de un individuo (*¿Qué es el phishing?*, 2022).

5.3.2. Organizaciones:

Para las organizaciones, el phishing es un peligro mayor ya que tal entrada puede resultar en la pérdida de información importante, incluyendo números de empleados y registros de clientes. Además, estos ataques pueden llevar directamente a pérdidas que son de naturaleza financiera, interrupción de las actividades empresariales y una mala reputación debido a la pérdida de confianza entre los clientes o con los socios comerciales (SPConnet, 2024).

5.4. Medidas de seguridad existentes

5.4.1. Protocolos de autenticación

5.4.1.1. Autenticación de dos factores (2FA)

La verificación de dos factores, que se ha vuelto casi universal en los últimos años y proporciona un nivel extra de seguridad a todos los sistemas de inicio de sesión, debe complementarse con un nombre de usuario y una contraseña. Por lo general, es la contraseña junto con un token temporal que se entregará al dispositivo del usuario incluso si la contraseña es filtrada o hackeada, lo que resulta en un proceso bastante complejo para hackear la cuenta de alguien (*10 medidas de seguridad en sitios web*, 2024).

5.4.1.2. Captcha

Los CAPTCHA existen para distinguir humanos de bots: crean tareas que son fáciles para los humanos, pero complejas para los bots. En reCAPTCHA, esto generalmente significa desafíos que requieren la selección de ciertos tipos de objetos, como carteles, en una colección de imágenes (*Captcha | reCAPTCHA Enterprise*, 2024).

5.4.2. Certificados SSL/TLS y cifrado de datos.

5.4.2.1. Certificados SSL/TLS

Un servidor web y un navegador pueden comunicarse de forma segura y cifrada, lo que se conoce como SSL (Secure Socket Layer) o su versión actualizada TLS (Transport Layer Security).

Los certificados SSL/TLS mantienen los datos seguros y privados entre usted y el sitio web, sin importar qué tipo de información se esté enviando, ya sean sus credenciales de inicio de sesión o su número de casa, a través de una conexión de Internet segura (*¿Qué son SSL, TLS y HTTPS?*, 2022).

5.4.2.2. Cifrado de datos

La información es solo un revoltijo de hojas que caen sin una clave, basura. Estos son también un conjunto fundamental de métodos para proteger los datos en reposo, y todos caen bajo el paraguas de lo que se considera datos en movimiento. Así que no importa lo que pase, o si alguien obtiene acceso a su información, no podrían usarla en su contra.

5.4.3. Detección y Monitoreo de Actividades Maliciosas.

5.4.3.1. Monitoreo continuo

Si la actividad de sus sitios está suficientemente supervisada, se puede detectar cualquier actividad sospechosa en tiempo real e incluso tomar medidas contra las que parezcan maliciosas. Si bien una detección específica no necesariamente se correlaciona con que las herramientas de monitoreo sean efectivas para detectar amenazas, organizaciones como la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) abogan por el uso de herramientas que monitorean su entorno como un esfuerzo para mejorar la conciencia de su organización y la capacidad de arrancar la tirita de una potencial amenaza si ocurre.

5.4.3.2. Sistemas de Detección de Intrusiones (IDS)

Los IDS monitorean el tráfico de la red en busca de patrones que indiquen intentos de acceso no autorizado o actividad maliciosa. Debido a que la fuente del texto buscado no está claramente identificada, es de conocimiento común en la seguridad de dominios que los IDS deben utilizar paquetes de datos forenses como parte integral de los protocolos criptográficos.

5.5. Contexto en Ecuador

5.5.1. Escenario de Phishing en Ecuador.

Los últimos años el Ecuador ha sido testigo de un inquietante aumento en los ataques de phishing. El Ecuador posee el mayor número de ataques de phishing y se ha visto el mayor incremento de este tipo de ataques este último año (*Ecuador encabeza el listado de países en la región con más ataques de phishing*, 2023).

Según los datos que proporciona Kaspersky, el phishing aumentó un 140 % en América Latina durante este periodo, totalizando 397 millones de bloqueos. Ecuador se encuentra entre los cinco países a nivel regional que reportan estos mensajes (*Aumentan en 140% las estafas mediante mensajes falsos en América Latina, revela Kaspersky*, 2024).

5.5.2. Nivel de adopción de medidas de seguridad en sitios web locales.

Falta información específica; sin embargo, la creciente amenaza de ciberataques ha causado que varias organizaciones locales en Ecuador inicien el fortalecimiento de sus protocolos de seguridad. Pero diferentes instituciones tienen diferentes prácticas: algunas utilizan autenticación multifactor (MFA), tienen certificados SSL/TLS y tienen sistemas de monitoreo continuo. Para las instituciones ecuatorianas, es un enfoque orientado al futuro y no pueden pasar por alto la necesidad de protegerse contra phishers y otras amenazas cibernéticas.

5.5.3. Leyes y Regulaciones sobre Protección de Datos

El avance en la protección de datos y las disposiciones de la Ley Orgánica de Protección de Datos Personales ayudan a proteger los datos personales de la gran mayoría de las personas en Ecuador.

VI. MARCO METODOLÓGICO

En esta investigación se emplea un enfoque cualitativo, ya que permite analizar en detalle el impacto del phishing en la seguridad de los sitios web en Ecuador. Para ello, se revisa información documental, estudios previos y casos relevantes, con el objetivo de interpretar el problema desde diferentes perspectivas.

El estudio sigue un diseño de investigación no experimental, de tipo descriptivo y exploratorio. Esto significa que no se manipulan variables, sino que se examinan diversas fuentes secundarias, como informes de seguridad, artículos académicos y estudios de caso, para obtener una comprensión amplia del tema.

La información se recopila a través del análisis de documentos y reportes especializados sobre incidentes de phishing. Se busca identificar los patrones y estrategias que utilizan los ciberdelincuentes, así como las medidas que se han implementado para hacer frente a estos ataques.

Por último, los hallazgos se interpretan considerando el contexto actual del phishing en Ecuador. Con base en este análisis, se plantean recomendaciones que pueden ayudar a mejorar la seguridad de los sitios web y reducir su vulnerabilidad ante este tipo de amenazas.

VII. RESULTADOS

El análisis de los controles de seguridad contra ataques de phishing revela la importancia de implementar medidas efectivas para mitigar los riesgos asociados a este tipo de amenazas.

Una de las más utilizadas es la autenticación multifactor, ya que proporciona una capa adicional de seguridad al momento de requerir más de una forma de verificación antes de conceder acceso a una cuenta. Esta medida demuestra ser altamente efectiva en la reducción de accesos no autorizados, aunque algunas variantes, como el uso de códigos por SMS, pueden ser vulnerables a ataques como el intercambio de SIM.

Otra medida es el uso de certificados SSL/TLS, los cuales nos garantizan una comunicación segura entre los usuarios y los sitios web. El cifrado de datos protege la información transmitida y refuerza la confianza de los usuarios en las plataformas digitales. Sin embargo, es importante considerar que un certificado SSL expirado puede generar advertencias en los navegadores, lo que podría afectar la credibilidad de un sitio web.

El correo electrónico sigue siendo uno de los vectores más utilizados en ataques de phishing. Por ello, la implementación de protocolos de seguridad como SPF, DKIM y DMARC es crucial para evitar la suplantación de identidad y reducir el número de correos fraudulentos que llegan a los usuarios. Estos protocolos han demostrado ser efectivos en la autenticación de correos legítimos y en la mitigación de ataques de phishing a gran escala.

Los sistemas de seguridad en red, como los firewall y las soluciones de detección y prevención de intrusiones, desempeñan un papel importante en la protección contra estas amenazas cibernéticas. Estos sistemas analizan el tráfico en busca de patrones maliciosos y bloquean intentos de ataque antes de que puedan causar daño. No obstante, requieren actualizaciones y

mantenimiento continuo para ser efectivos, ya que los métodos de ataque evolucionan constantemente.

La concienciación y educación de los usuarios es otro aspecto fundamental en la lucha contra el phishing. Muchas víctimas caen en estos ataques debido a la falta de conocimiento sobre cómo identificar correos y sitios web fraudulentos. La implementación de programas de formación en ciberseguridad, junto con simulaciones de ataques de phishing, permite fortalecer la capacidad de detección de los usuarios y reducir la efectividad de estas amenazas.

El análisis de vulnerabilidades y la aplicación de parches de seguridad tienen un papel importante en la protección de sistemas y aplicaciones. Las auditorías constantes permiten identificar brechas de seguridad antes de que puedan ser explotadas por ciberdelincuentes. Sin embargo, es importante considerar que algunas actualizaciones pueden generar problemas de compatibilidad con otros sistemas, por lo que deben ser implementadas con precaución.

Un enfoque integral de seguridad también requiere la monitorización y respuesta a incidentes en tiempo real. Los equipos de ciberseguridad que operan en centros de operaciones de seguridad (SOC) pueden detectar y mitigar ataques de manera rápida y eficiente. La inversión en tecnología y personal especializado permite minimizar el impacto de los incidentes de seguridad y mejorar la resiliencia de las organizaciones frente a ataques de phishing.

El factor humano sigue siendo una de las principales vulnerabilidades en la seguridad digital. Los ataques de phishing no solo dependen de la tecnología y el ingenio de los atacantes, sino también de la manipulación psicológica de la víctima. La implementación de estrategias de concienciación sobre ingeniería social es esencial para reducir el éxito de estos ataques. Como

capacitar a los usuarios para que reconozcan tácticas como la suplantación de identidad y la urgencia falsa puede marcar una diferencia significativa en la prevención del phishing.

Las estrategias para mitigar los ataques de phishing han evolucionado debido a la creciente sofisticación de estas amenazas. Para reducir las posibilidades de acceso no autorizado y robo de identidad, es fundamental implementar medidas de seguridad estrictas.

En servicios cruciales como plataformas bancarias, gubernamentales y de comercio electrónico, la autenticación de dos factores (2FA) debe ser un requisito obligatorio. Esto implica la configuración de sistemas de autenticación que utilicen factores independientes, como aplicaciones autenticadoras o llaves de seguridad físicas, en lugar de códigos SMS, los cuales son vulnerables al intercambio de SIM.

La educación y concienciación de los usuarios es una de las defensas más efectivas contra el phishing. Se deben desarrollar programas de formación en ciberseguridad para empleados y estudiantes, campañas de concienciación sobre nuevas técnicas de phishing y simulaciones prácticas de ataques para evaluar la capacidad de detección de los usuarios. En el ámbito corporativo, enviar correos electrónicos simulados de phishing permite medir cuántos empleados caen en la trampa y proporcionar asesoramiento personalizado para mejorar su capacidad de respuesta. Además, los incentivos pueden reforzar un comportamiento seguro dentro de las organizaciones.

Dado que los correos electrónicos son uno de los vectores de ataque más utilizados en el phishing, es esencial implementar protocolos de seguridad como DMARC, SPF y DKIM para evitar el uso fraudulento de correos electrónicos corporativos. Se debe configurar un registro SPF que indique qué direcciones IP están autorizadas a enviar correos en nombre de la organización,

utilizar DKIM para firmar digitalmente los correos y establecer una política DMARC que indique qué hacer con los mensajes sospechosos.

La seguridad de los sitios web también es clave para prevenir el phishing. Es imprescindible adquirir certificados SSL/TLS para garantizar que todos los sitios usen HTTPS, desplegar protocolos de Seguridad Rígidos de Transporte HTTP (HSTS) para evitar ataques de degradación de HTTP, y utilizar cortafuegos basados en host, así como sistemas IDS/IPS que bloqueen conexiones no autorizadas.

El marco legal y normativo también juega un papel crucial en la protección contra el phishing. Las empresas e instituciones deben ser responsables de la seguridad de sus sistemas, asegurando actualizaciones regulares y auditorías de seguridad. Se deben establecer requisitos mínimos de protección para quienes procesan datos personales o financieros y desarrollar auditorías internas y externas para identificar vulnerabilidades. Incentivar a las empresas con beneficios fiscales o certificaciones por implementar buenas prácticas de seguridad fomenta una cultura de ciberseguridad más sólida. Finalmente, la cooperación con organizaciones de ciberseguridad y la creación de mecanismos de reporte para incidentes de phishing permiten una respuesta rápida y efectiva ante nuevas amenazas.

VIII. DISCUSION DE LOS RESULTADOS

Las estrategias de seguridad son clave para mitigar ataques de phishing. La autenticación multifactor (MFA) reduce accesos no autorizados, aunque el uso de SMS sigue siendo vulnerable a ataques de intercambio de SIM, por lo que se recomienda el uso de llaves físicas o aplicaciones autenticadoras. Los certificados SSL/TLS garantizan conexiones seguras, pero su caducidad puede afectar la confianza del usuario. Para evitar esto, es fundamental su renovación automática y la aplicación de HSTS.

En seguridad de correos electrónicos, SPF, DKIM y DMARC ayudan a prevenir la suplantación de identidad, aunque su implementación sigue siendo un reto en muchas organizaciones. Los firewalls y sistemas IDS/IPS detectan y bloquean ataques, pero requieren actualizaciones constantes y monitoreo continuo, algo que no siempre es viable por falta de recursos.

La concienciación del usuario es fundamental, ya que muchas víctimas caen en ataques de phishing por desconocimiento. Programas de capacitación y simulaciones han demostrado ser efectivos, pero requieren actualización constante. El análisis de vulnerabilidades y la aplicación de parches son esenciales, aunque algunas actualizaciones pueden generar problemas de compatibilidad, por lo que deben ser probadas antes de su implementación.

Los centros de operaciones de seguridad (SOC) han demostrado ser efectivos en la respuesta a incidentes, pero muchas organizaciones carecen de recursos para su implementación, lo que podría resolverse con iniciativas gubernamentales y alianzas estratégicas.

El factor humano sigue siendo la mayor debilidad en la seguridad. Los ataques de phishing explotan la manipulación psicológica, por lo que es vital reforzar la educación en ingeniería social e incentivar prácticas seguras en las organizaciones.

Para combatir eficazmente el phishing, se requiere un enfoque integral que combine tecnología, educación y regulaciones. Empresas y usuarios deben adoptar medidas de protección proactivas para enfrentar un entorno de amenazas en constante evolución.

IX. CONCLUSIONES

Se evaluó el estudio del phishing ya que es una amenaza creciente en Ecuador, esto evidencia la alta incidencia de fraude digital y la necesidad de fortalecer la seguridad en línea. Además, la falta de conocimiento sobre phishing y medidas de protección eficaces incrementa la vulnerabilidad de los usuarios y organizaciones.

Se estableció diversas medidas de seguridad esenciales para prevenir ataques de phishing en sitios web. Entre las más efectivas se encuentran la autenticación multifactor (2FA), el uso de certificados SSL/TLS para cifrar la comunicación, la implementación de firewalls y sistemas de detección de intrusos (IDS), así como la configuración de protocolos de seguridad en correos electrónicos (SPF, DKIM y DMARC). Además, se destacó la importancia de la concienciación y educación en ciberseguridad como un factor clave para reducir la vulnerabilidad de los usuarios ante ataques de phishing. Sin embargo, la adopción de estas medidas en Ecuador aún es limitada, lo que subraya la necesidad de promover su implementación en empresas y organizaciones para fortalecer la seguridad de los sitios web.

Se describieron los principales controles utilizados para mitigar ataques de phishing en sitios web. Entre ellos, la autenticación multifactor (MFA) se destacó como una barrera efectiva para evitar accesos no autorizados. Los certificados SSL/TLS garantizan la integridad y confidencialidad de la información transmitida, mientras que los sistemas de detección de intrusos (IDS/IPS) permiten identificar y bloquear intentos de ataque en tiempo real. En el ámbito del correo electrónico, protocolos como SPF, DKIM y DMARC ayudan a prevenir la suplantación de identidad y la entrega de correos maliciosos. A pesar de la eficacia de estos controles, su implementación sigue siendo desigual, lo que deja brechas de seguridad que pueden ser aprovechadas por atacantes.

Se propuso estrategias de seguridad para prevenir los ataques de phishing en los sitios web. Entre las soluciones planteadas se encuentran la implementación obligatoria de 2FA en plataformas críticas, el desarrollo de programas de capacitación en ciberseguridad para usuarios y empresas, y la mejora en la detección de ataques mediante el uso de inteligencia artificial y machine learning. Además, se destaca la importancia de la cooperación entre el sector público y privado para fortalecer la ciberseguridad a nivel nacional.

X. RECOMENDACIONES

Se recomienda la implementación de campañas de concienciación sobre phishing en instituciones educativas, empresas y organismos gubernamentales. Estas capacitaciones deben centrarse en la identificación de correos fraudulentos, enlaces sospechosos y prácticas seguras en internet.

Dado que el phishing busca acceder a las credenciales, se ha vuelto una necesidad implementar el uso activo de la autenticación de dos factores (2FA), lo cual sería de extrema importancia en todas las plataformas digitales, pero especialmente en aquellas que manejan datos pagos/sensibles o tienen un objetivo específico.

Específicamente, se recomienda que las empresas utilicen certificados SSL o TLS para asegurar sus conexiones. Sin embargo, el IDS (Sistema de Detección de Intrusiones) es otra medida que podría reducir aún más la exposición de las empresas a estos ataques, ya que permite monitorear actividades sospechosas en su plataforma.

Es fundamental que el país refuerce las leyes sobre seguridad informática, promoviendo auditorías de ciberseguridad en empresas y a las entidades gubernamentales. Esto garantizará la adopción de prácticas de protección de datos y reducirá la vulnerabilidad ante ataques de phishing.

XI. REFERENCIAS

10 medidas de seguridad en sitios web. (2024, marzo 4). https://ocean-theme.com/es/blog/10-medidas-de-seguridad-en-sitios-web

Aumentan en 140% las estafas mediante mensajes falsos en América Latina, revela Kaspersky. (2024, octubre 15). /. https://latam.kaspersky.com/about/press-

releases/aumentan-en-140-las-estafas-mediante-mensajes-falsos-en-america-latina-revela-kaspersky

BBVA. (2025, enero 30). *BBVA ESPAÑA*. https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-sim-swapping.html

Benítez, D. J. P. (2021). *SECRETARIA GENERAL JURÍDICA*.

Campillo, R. (2022, febrero 18). Qué es el SIM Swapping y cómo evitar el fraude. *Mobbeel*. https://www.mobbeel.com/blog/que-es-el-sim-swapping-y-como-evitar-el-fraude/

Captcha | *reCAPTCHA Enterprise*. (2024, diciembre 5). Google Cloud. https://cloud.google.com/recaptcha/docs/captchas?hl=es-419

¿Cómo identificar un correo electrónico de phishing?-Comunidad Huawei Enterprise. (2024, julio 31). https://forum.huawei.com/enterprise/intl/es/thread/%C2%BFC%C3%B3mo-identificar-un-correo-electr%C3%B3nico-de-phishing/815175127288090624?blogId=815175127288090624

Cómo identificar y eliminar ventanas emergentes falsas: Todo lo que necesitas saber. (2019, noviembre 8). /. https://www.kaspersky.es/resource-center/threats/identify-and-remove-fake-pop-ups

¿Cuáles Son los Distintos Tipos de Phishing? (2021, junio 9). Trend Micro. https://www.trendmicro.com/es_mx/what-is/phishing/types-of-phishing.html

Ecuador encabeza el listado de países en la región con más ataques de phishing. (2023, noviembre 7). Primicias. https://www.primicias.ec/noticias/tecnologia/ecuador-deteccion-ataques-phishing/

Pharming: Protección contra la redirección a sitios web fraudulentos. (2020, febrero 11). IONOS Digital Guide. https://www.ionos.mx/digitalguide/correo-electronico/seguridad-correo-electronico/que-es-el-pharming/

¿Qué es el phishing? | *Seguridad de Microsoft*. (2022, julio 22). https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing

¿Qué es el ransomware? | *IBM*. (2024, junio 4). https://www.ibm.com/mx-es/topics/ransomware

¿Qué es el whale phishing? | *IBM*. (2023, abril 25). https://www.ibm.com/mx-es/topics/whale-phishing

¿Qué es phishing? - Definición, ejemplos de ataques y más | *Proofpoint ES*. (2022, marzo 24). Proofpoint. https://www.proofpoint.com/es/threat-reference/phishing

¿Qué es Smishing y cómo protegerse? ✉ [+7 Ejemplos]. (2023, junio 27). https://www.deltaprotect.com/blog/smishing-que-es

¿Qué es un ataque de gemelo malvado y cómo actúa? (2023, diciembre 4). ¿Qué es un ataque de gemelo malvado y cómo actúa? https://www.avast.com/es-es/c-evil-twin-attack

¿Qué es un ciberataque y los tipos de ataques en la red? (2022, febrero 26). Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks.html

¿Qué son SSL, TLS y HTTPS? | *DigiCert*. (2022, abril 7). https://www.digicert.com/es/what-is-ssl-tls-and-https

Quishing: Understanding the threats behind QR codes | *Phriendly Phishing Blog*. (2024, octubre 9). https://www.phriendlyphishing.com/blog/qrshing-understanding-the-threats-behind-qr-codes

Sayago-Heredia, J. (2021). Ciberseguridad en Ecuador y Latinoamérica. *Killkana Técnica*, *5*(1). https://doi.org/10.26871/killkanatecnica.v5i1.957

SPConnet. (2024, agosto 27). El Impacto del Phishing en las Empresas y Cómo Prevenirlo: Análisis de Casos y Estrategias de Prevención. *SPConnet*. https://spconnet.com/impacto-phishing-empresas-estrategias-prevencion/

Tipos de malware y ejemplos. (2017, octubre 17). /. https://latam.kaspersky.com/resource-center/threats/types-of-malware?srsltid=AfmBOop8iqAUBga2TGESDuBRWHU2XQptBDzQc3Nnjqkl8lIM9ZycqaC8&utm_source=chatgpt.com

What Is a Watering Hole Attack? (2021, febrero 23). Fortinet. https://www.fortinet.com/resources/cyberglossary/watering-hole-attack

XII. ANEXOS

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE SISTEMAS DE INFORMACIÓN

Babahoyo, 13 de marzo de 2025

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación del Sr.: **HECTOR EDUARDO SILVA CHICHANDE**, cuyo tema es: **IMPACTO DE LAS TÉCNICAS DE PHISHING EN LA SEGURIDAD DE SITIOS WEB**, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de **[7%]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.

Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

JOSE DANILO VILLARES PAZMIÑO

Ing. José Danilo Villares Pazmiño, Mg.
DOCENTE FAFI.